Dedicated to Global First Responders

CBRNE NEWSLETTER TERRORISM

June 2017

London Bridge

Borough Market

Westminster Bridge

Manchester Arena

www.cbne-terrorism-newsletter.com

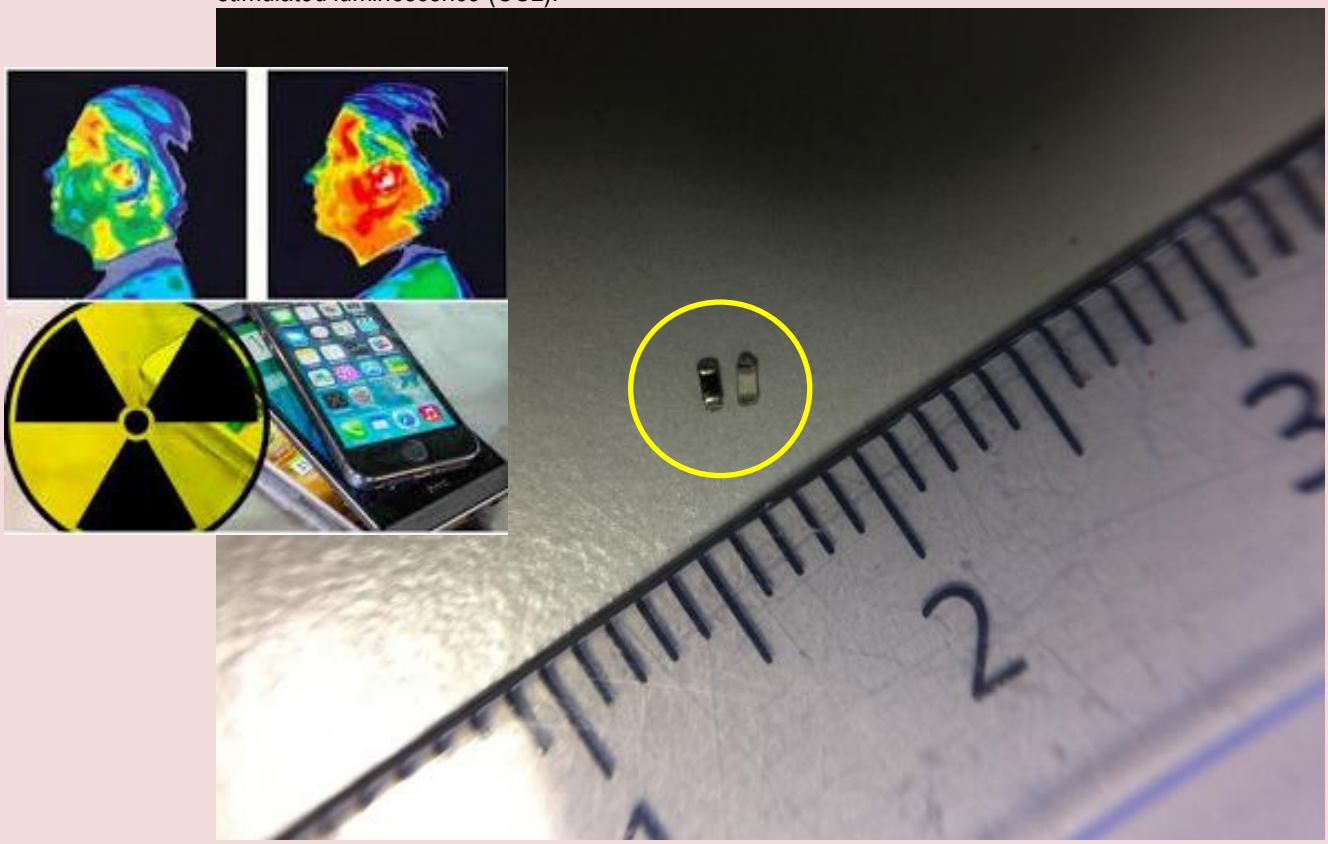

ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
DIRTY R-NEWS

Mobile phones can reveal exposure to radiation

Source: http://www.homelandsecuritynewswire.com/dr20170526-mobile-phones-can-reveal-exposure-to-radiation

May 26 – The nuclear power plant disasters in Chernobyl and Fukushima are two examples of accidents which have exposed the population to ionizing radiation. Many people fear that, for example, dirty bombs will be used in future terror attacks.
"Being able to quickly determine whether someone has been exposed to radiation is a major advantage. In case of a nuclear power plant disaster, many people are worried, even when only a small number of people have been exposed to harmful levels of radiation", explains Therése Geber-Bergstrand, medical physicist and doctoral student at Lund University.

Providing information several years after an accident
Together with her colleagues, Geber-Bergstrand examined a number of objects or materials that come in close contact with the body and which have the potential of providing information on whether the carrier has been exposed to radiation. Among the objects examined were:
— mobile phones
— teeth and dental fillings
— drying agents (found in, for example, small pouches in new brief cases and purses)
Lund says that the study showed that several of the materials contained very promising properties, not least mobile phones. They contain resistors made from aluminum oxide, which can provide information about radiation as late as six years after the time of exposure. During analysis, the phone is dismantled and the resistor is subsequently examined using a light-sensitive measuring technique, known as optically stimulated luminescence (OSL).



Mobiles contain resistor made from aluminium oxide, which can provide information about radiation as late as six years after the time of exposure.

"The results from the mobile phones were very promising. Even though further studies are required, the phones can be used right away. We have an agreement with the Swedish Radiation

Safety Authority about analyzing a number of mobile phones in our emergency preparedness lab when needed", says Geber-Bergstrand.
Analyses of mobile phones and of other tested objects can also be performed on a large scale and relatively quickly. It may be possible to receive a test result within one or two hours, compared to the couple of days it can take to receive tests results from a medical exam. According to Geber-Bergstrand, an initial check of the mobile phone can therefore be a valuable tool for determining who needs to undergo more time-consuming and resource-intensive tests.

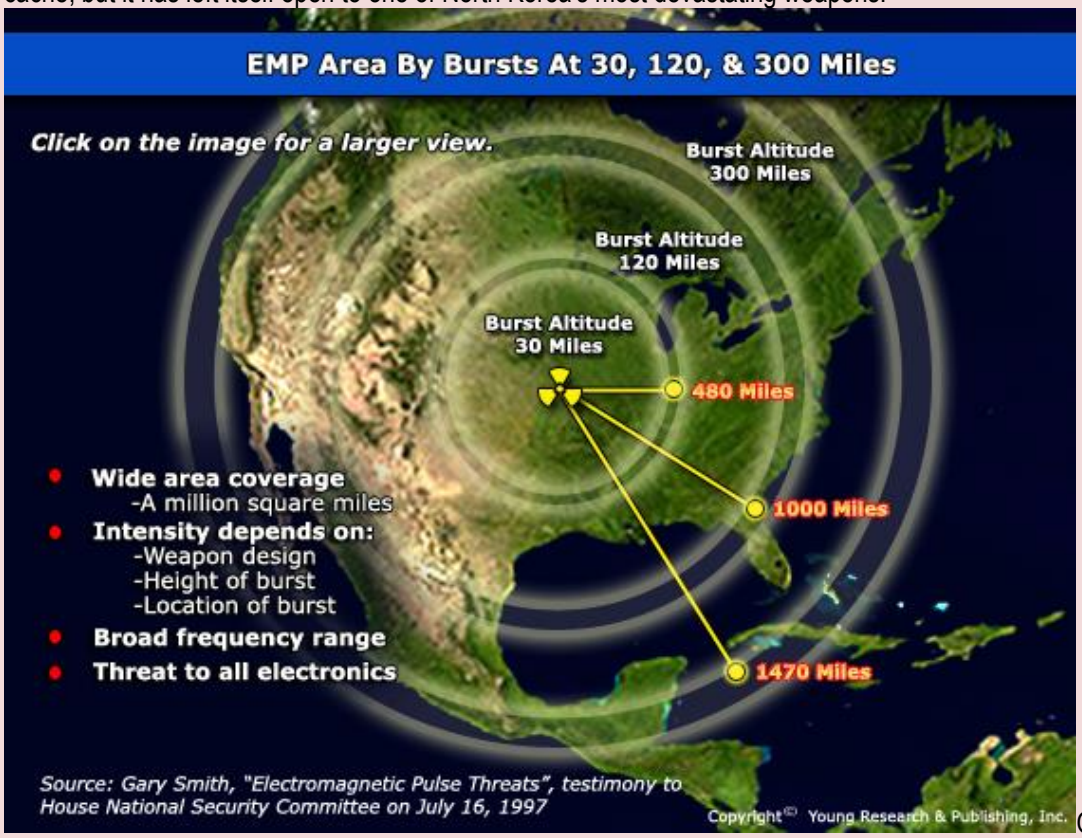
Salt capsules could complement dosemeters
In her thesis, she also continued to develop the research group's previous findings with regard to the use of table salt as a cheap and effective indicator of ionizing radiation. Her results confirm the benefits of the salt. In the event of a major accident involving radioactive substances, it could therefore be an option to supply some of the emergency staff with special salt capsules as an effective and cheap alternative to dosemeters.

— Read more in Therése Geber-Bergstrand,Optically Stimulated Luminescence for Retrospective Radiation Dosimetry. The Use of Materials Close to Man in Emergency Situations (Ph.D. dissertation, Lund University; 2017).

North Korea's Silent, Invisible WMDs That No One's Talking About

Source: https://moneymorning.com/2017/06/02/north-koreas-silent-invisible-wmds-that-no-ones-talking-about/

June 02 – The U.S. military has been working double time to upgrade its traditional-warfare weapons cache, but it has left itself open to one of North Korea's most devastating weapons.



On May 2, the U.S. military announced that its South Korea-based THAAD missile defense system was fully operational and ready to thwart any mid-range missile attacks Pyongyang may launch on U.S. allies in the East.
And just this past Tuesday (May 29), the U.S. military cheered its first successful missile defense test involving a simulated attack by an intercontinental ballistic missile (ICBM).

But these lauded advancements may be overshadowing the reality of another threat Pyongyang poses… This threat is silent, invisible, and potentially more menacing than nuclear bombs. ***Money Morning*** Executive Editor Bill Patalon says its aftermath could "alter the American way of life – without the accompanying 'on switch' to put things right again."

We're talking about an electromagnetic pulse (EMP) attack.

Here's what you need to know about this "silent weapon of mass destruction" and how it's largely being ignored by politicians and analysts – to the American public's detriment.

We're Not Prepared for EMP Attacks

First, it's important to know that we're exposed to different types of EMPs every day – from power line surges, electric motors, and continual switching actions of electronic circuitry.

But EMP *attacks* would instantaneously expose us to electromagnetic pulses hundreds of thousands of times stronger than those emitted by everyday electronic devices.

Specifically, an EMP attack surge would short electrical devices for hundreds of miles around us. It wouldn't just disable our cell phones – our industrial computer servers, transformers, and city/regional circuit breaker panels would be rendered useless as well. Rolling blackouts would ensue, encompassing entire multistate regions of the United States.

"Think about these horrors," Bill says. "Any passenger jet flying within range would crash, killing everyone on board; anyone on ventilators or other forms of life support would die, because even the backup system would fry; cities would gridlock from *all* the traffic control systems crashing. It would be like the Great Northeast Blackout – on steroids."

Indeed, such an attack would be extremely chaotic to the United States – a nation almost wholly dependent upon electricity.

Not to mention that we have done nothing to shield our electrical grid from a North Korean EMP attack.

"Our devices – *all* of our electrical devices – aren't shielded from this kind of attack," Bill says.

And to this point, former Speaker of the House Newt Gingrich admitted as much in a ***FOX News*** op-ed just this morning: "[The U.S. electrical] grid is ill-prepared to handle [an EMP attack]," he wrote.

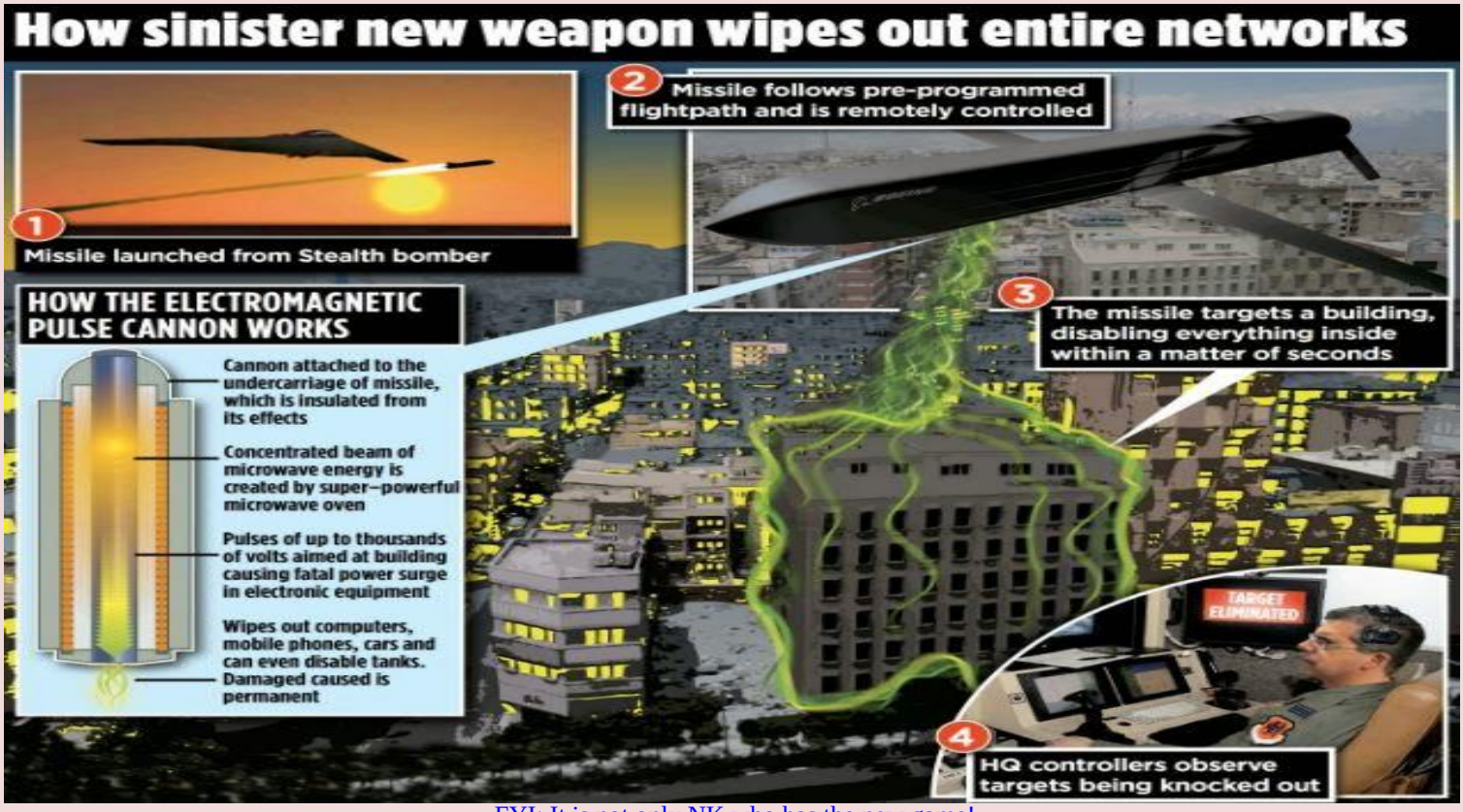
Gingrich went on to talk about how he had taken his North Korea EMP attack warning to Congress about a month ago on May 4. He told members of the U.S. Senate that the government needs to do something about its electrical vulnerabilities – now.

For example, Uncle Sam could take advantage of an invention two University of Nebraska engineers revealed last November: a cost-effective concrete mix that acts as a shield against intense pulses of electromagnetic energy. If coated on the outside of large buildings, all electrical devices within would be protected from a large-scale EMP emission.

Gingrich also wrote that he'd told the Senate to "cut red tape" to allow such kinds of engineer-based innovations to be used.

But Gingrich was largely ignored by his peers, which could explain why he used a *FOX News* op-ed as the medium to share his message today.

In fact, if EMP attack warnings like Gingrich's aren't being ignored by politicians and experts, then they're being outright denied…



FYI: It is not only NK who has the new game!

EMP Attacks Come in Many "Shapes and Sizes"

For example, Jack Liu and Jeffrey Lewis, both Asia-specific nuclear non-proliferation analysts, wrote off the possibility of a North Korean EMP attack on May 10. They told *VICE News* that it was "unlikely science fiction" because the 10- to 20-kiloton nuclear weapons currently possessed by Pyongyang aren't capable of producing an effective EMP pulse.

But just this morning, Dr. William R. Graham, former science advisor to President Ronald Reagan, told *38 North* readers that Liu and Lewis' dismissals were irresponsible. He argued that they had failed to provide thorough, concrete analysis of the two main forms atmospheric EMP attacks can take.

These forms are:

- **Super-EMP attacks:** These attacks are low-yield explosions designed to generate frequencies compact and powerful enough to knock out all electrical devices in a concentrated (though large) area (i.e., the continental United States). Graham told ***38 North*** that Pyongyang's previous nuclear tests had resulted in damage yields consistent with Super-EMP attacks.
- **Satellite EMP attacks:** These attacks don't require long-range ICBMs to deliver a nuclear warhead to space. Instead, as Graham wrote, these attacks would be carried out "by launching a short-range missile off a freighter or submarine or by lofting a warhead to 30 kilometers burst height by balloon." He explained that "while such lower-altitude EMP attacks would not cover the whole U.S. mainland, as would an attack at higher altitude (300 kilometers), even a balloon-lofted warhead detonated at 30 kilometers altitude could black out the Eastern Grid that supports most of the population and generates 75% of U.S. electricity."

To add to the atmospheric forms, Bill says that EMP attacks can also take place on land in the form of surface EMP attacks…

"An EMP weapon could be trucked in, brought into a harbor by boat or sub, or flown in," he explains.

Surface EMPs are ground-based bursts of electromagnetic waves inflicted to render a specific area powerless. Their damage ranges are considerably smaller than atmospheric EMP attacks, but their delivery weapons are easier to conceal.

Whichever form a North Korean EMP attack takes, the damage inflicted will largely reflect upon the nation's preparation ahead of time (or lack thereof).

And Bill says it's best not to wait for Uncle Sam to make that first move…

Protect Your Future Selves Now

As an expert of the "Asian Arms Race" and an analyst who's been eyeing North Korea's nontraditional weapons advancements for several years, Bill knows that it would be tough to consider your finances amid the devastating aftermath of a WMD attack. And he understands that some members of the public don't necessarily see a point in securing their financial futures when "planes are falling out of the sky."

But in the wake of any attack – or of any widespread disaster, for that matter — fiscal security provides a much-appreciated added layer of protection.

So Bill still says investors ought to keep their future selves in mind…

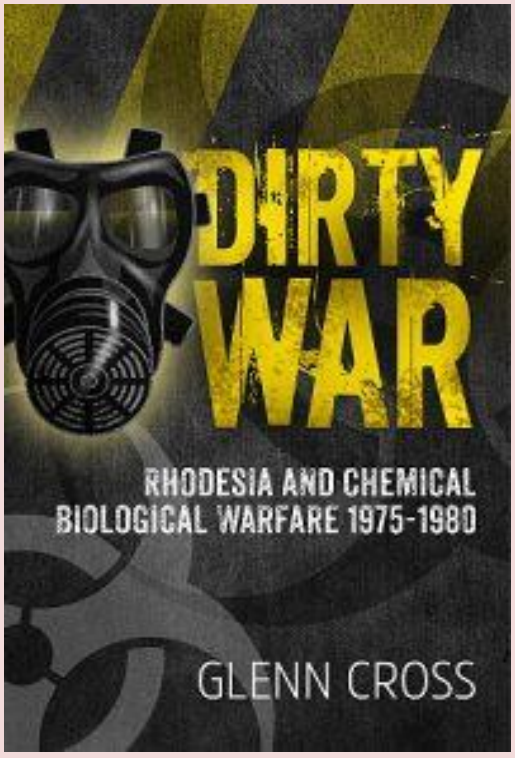
He recommends **Lockheed Martin Corp.** (NYSE: LMT), for example. On Tuesday, March 29, missile defense experts at Lockheed were officially tasked with building between 18 and 40 missile rocket interceptors to protect against incoming ballistic missile threats. That contract was worth $273.5 million.

And since Bill first recommended Lockheed in March 2016, its share price has gone up 26%.

Did 'dirty war' tactics kill more guerrillas in Rhodesia than conventional?

Source: http://blog.helion.co.uk/did-dirty-war-tactics-kill-more-guerrillas-in-rhodesia-than-conventional-military-units/

June 01 – Although some nations have developed or acquired chemical or biological agents, few have ever used these weapons against their adversaries. One of the few



countries ever thought to have used chemical or biological agents was Rhodesia. This small, landlocked breakaway British colony in Southern Africa used chemical and biological agents during its protracted struggle against an increasingly numerous African nationalist insurgency in the years following Rhodesia's Unilateral Declaration of Independence (UDI) from Britain in November 1965.

The genesis of the Rhodesian Chemical Biological Warfare (CBW) effort was to be found in the deteriorating security situation that developed following Mozambique's Independence from Portuguese colonial rule after the 25 April military coup d'état in Lisbon and the subsequent 'Carnation' revolution. The rise of the Frente de Libertação de Moçambique (FRELIMO) in Mozambique effectively forced the overstretched and under-resourced Rhodesians to defend their long land border with Mozambique – effectively a second front.

During the Rhodesian war, Rhodesian Security Forces were far better trained and equipped than their guerrilla adversaries. In a pitched battle between the Rhodesian Security Forces and guerrillas, the guerrillas usually lost. For that reason, guerrillas typically avoided contact with Rhodesia military

or police units – seeking instead to ambush soft, largely civilian targets (i.e. isolated farmhouses, rural schools, district commissioners, veterinary workers and civilians travelling on the roads).

Later in the struggle, the Rhodesians (facing severe manpower and materiel shortages) adopted unconventional tactics or techniques against a foe that fled rather than fight – including the use of recruited agents to **insert CBW-contaminated food, beverages, medicines and clothing into guerrilla supplies.** Some of these supplies were provided to guerrilla groups inside Rhodesia; some were transported to guerrilla camps in Mozambique. In all, deaths attributed to CBW agents often exceeded the monthly guerrilla body count claimed by conventional Rhodesian military units – demonstrating the utility of CBW agents in a counterinsurgency campaign against an elusive enemy.

Although few details are known about Rhodesia's clandestine CBW efforts, a broad-brush picture is clear. The project was born out of desperation as the conflict intensified in the mid-1970s, and was the brainchild of a professor, Robert Symington, at the University of Rhodesia's medical school. He reportedly put forward the idea to the then-Minister of Defense, who advocated it to the Prime Minister. The Prime Minister – almost certainly in consultation with his War Cabinet – delegated responsibility to the Central Intelligence Organisation (CIO), and implementation was assigned to the Special Branch liaison component in the Selous Scouts. Although they were aware of the CBW program's existence, the full extent to which the Rhodesian political and military leadership was involved in the effort is obscure, due to the lack of documentary material or living witnesses.

Prime Minister Ian Smith publicly denied any knowledge of the program, but almost certainly approved the program's creation – even if he was not aware of the details of its daily operations. In December 1998, a Zimbabwe newspaper quoted Ian Smith as saying: 'It's a lot of rubbish. I know nothing about [such germ warfare]. They [the Rhodesian Security Forces] could have done so without my knowledge… Those saying that are giving us credit for being more creative and brilliant than what we were'.

Chief of Rhodesia's CIO, Ken Flower, was very aware of the CBW activities, having received bi-weekly status reports on the effort from McGuinness. The police (BSAP) commissioners – first Sherren, and later, Allum – were briefed on the CBW efforts, and at least Sherren took steps to ensure that the program remained concealed. In 1977, McGuinness briefed the Combined Operations (COMOPS) – headed by Lieutenant General Peter Walls – about the CBW effort.

Rhodesian Special Forces (Selous Scout) commander Lieutenant Colonel Ron Reid-Daly also knew of the CBW effort, and many of his men were likely involved in disseminating the tainted materials. Most readily available information about the program is based on the half-truths, rumors, conjectures, anecdotes and myths that circulated around the officers' messes and pubs frequented by members of the Rhodesian Security Forces, however.

Although little specific information remains available about the Rhodesian CBW effort, what is indisputable is that its primary purpose was to kill guerrillas – whether they were recruits transiting to camps in Mozambique, or guerrillas operating inside Rhodesia. The CBW effort took on the guerrilla threat from three fronts: first, the effort aimed to eliminate guerrillas operating inside Rhodesia through contaminated supplies, either provided by contact men, recovered from hidden caches or stolen from rural stores; a second-order effect was to disrupt the relations between village supporters and the guerrillas. Secondly, the effort worked to contaminate water supplies along guerrilla infiltration routes into Rhodesia – forcing the guerrillas either to travel through arid regions and to carry more water and less ammunition, or travel with more ammunition but move through areas patrolled by Rhodesian Security Forces.

The CBW effort was made up of a rag-tag band of amateurs, working with makeshift equipment and readily available commercial materials. They developed the means to inflict casualties on insurgent forces beyond the capabilities of Rhodesia's professional conventional military.

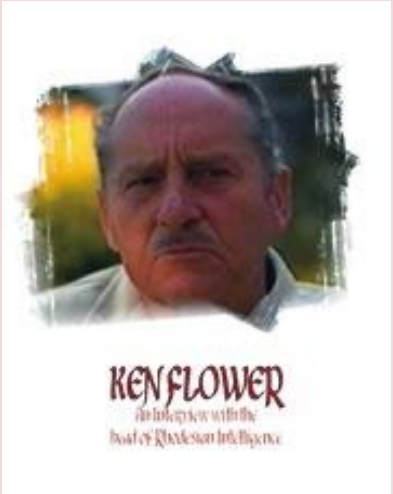
The chemical and biological agents developed by this small, rudimentary program were based almost exclusively on readily available toxic agricultural and industrial chemicals including warfarin (rodenticide), thallium (rodenticide), methyl parathion (an active ingredient in several organophosphate pesticides used in Rhodesia), Vibrio cholera (the causative agent of cholera), Bacillus anthracis (the causative agent of anthrax) and botulinum toxin. The Rhodesians may also have experimented with

several other agents – including ricin,13 abrin, amanita toxin, 2,4-dichlorophenoxyacetic acid (2,4-D), sodium fluoroacetate (compound 1080), cyanide, arsenic and tetra colchicine [sic] – but information on those experimental agents has proven hard to substantiate.

Of those knowledgeable insiders willing to talk, all share a consistent story about Rhodesia's development and use of chemical and biological agents during the Bush War; they even chillingly admit that chemical and biological agents were used in experiments on captured insurgents. In short, the story centres on an element of the BSAP Special Branch (attached to the Rhodesian Army's Selous Scouts), which implemented and oversaw the Rhodesian CBW effort from mid-to-late 1976 until late 1979.

The daily operation of this limited effort fell to a small Special Branch counterterrorist unit (sometimes referred to as 'Z Desk' or 'Counterterrorist Operations') under the command of Chief Superintendent Michael 'Mac' McGuinness. The Rhodesian CBW program was staffed with a small number of scientists and technicians working as 'consultants' to the Special Branch and co-located at the Special Branch/Selous Scout 'fort' outside Bindura (80 km north of Salisbury). The description of these insiders is instructive; it is one of a small band of scientists and students who served their 'call-ups' (often as long as three months) at the Bindura 'fort'.

The effectiveness of the Rhodesian poisons effort was constrained by its limited scope and application; the nature of the raw materials employed; and the crude dissemination methods. Nevertheless, participants in the poisons program saw it as hugely successful – at least early on. As mentioned earlier, **CIO Director-General Ken Flower** claimed in his autobiography that many hundreds of guerrillas were killed as a result of the poisons program; also mentioned earlier, the leadership saw the CBW effort – at least in its early days – as more effective than the conventional military. Symington echoed that sentiment. South African policeman Eugene de Kock stated: 'This [fact] confirmed that they [killed] a lot more of the enemy by means of the food and the clothing, than what they did in [daily] operations'. Most importantly, the 1977 Special Branch briefing to COMOPS opened by stating: '… The true extent of our success may never be known…' The report went on to claim 809 guerrilla deaths due to poisoning.



The most serious detriment to the project's continuing success was the guerrillas' eventual discovery of the program's activities, which made dissemination of poisoned items more difficult, as guerrillas became less trusting. Although the Special Branch continually devised new dissemination techniques, the growing guerrilla awareness of the poisoning effort did reduce the program's effectiveness. On this subject, the 28 June report stated: 'Our methods of operations are changing continually in order to keep the enemy guessing and [illegible] improved methods have recently come to light that bode well for the future'.

According to the scientific head of the CBW effort, Robert Symington, the Rhodesian poisoning program was very successful; some months it resulted in a greater number of guerrilla fatalities than the conventional military operations of the elite Rhodesian Light Infantry (RLI). This claim is plausible, given the reluctance of most guerrilla groups to engage conventional Rhodesian Security Forces in head-on battle; guerrilla bands preferred hit-and-run tactics against soft targets.

The only official Rhodesian assessment of the program's effectiveness is the estimate prepared for COMOPS. That paper estimates that, as of 28 June 1977, the poisoning program had resulted in the deaths of 809 individuals. Within SB circles at the time, it was widely believed that more guerrillas were dying from poison than from conventional Fireforce 'contacts'. Uncertainty remains whether the numbers briefed to COMOPS included estimates of deaths due to cholera. If not, the total for the CBW effort (including use of cholera) could be doubled.

► **Dirty War. Rhodesia and Chemical Biological Warfare 1975-1980 by Glenn Cross can be purchased** here.

A Closer Look at North Korea's Conventional Weapons

Source: https://geopoliticalfutures.com/closer-look-north-koreas-conventional-weapons/

June 2 – As Pyongyang, Washington and other regional players prepare for the prospect of war, North Korea's nuclear program and ballistic missile capabilities have received undue amounts of attention. Important though they may be, they have less bearing on how the war will be fought than does North Korea's conventional military.

Eliminating Pyongyang's nuclear capabilities would be the first objective in a war, and indeed the justification for an attack. The second objective would be to protect South Korea from North Korean retaliation. No one really knows the true status of Pyongyang's nuclear program, but a nuclear strike on a U.S. asset or ally is unlikely because it would force the U.S. to respond in kind, wiping out the North Korean regime.

North Korea will instead rely on its large arsenal of conventional weapons – namely artillery – to retaliate. The artillery batteries, many of which are located near the demilitarized zone, can severely damage heavily populated areas in and around Seoul.

Why there's no modern guide to surviving a nuclear war?

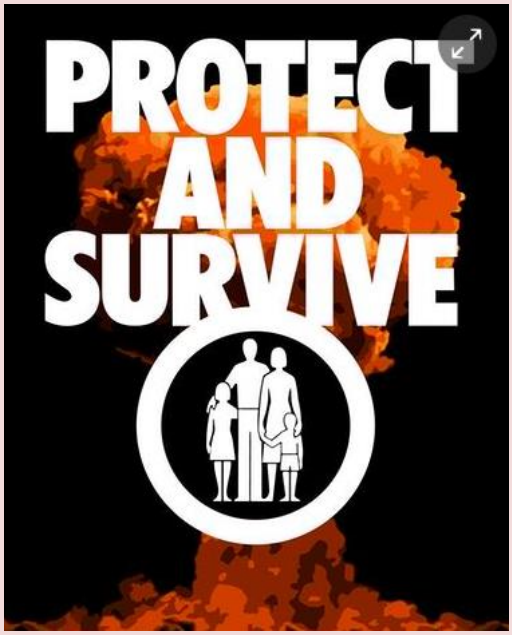
By John Preston

Source: http://www.homelandsecuritynewswire.com/dr20170609-why-there-s-no-modern-guide-to-surviving-a-nuclear-war

June 09 – The risk of thermonuclear war has rarely been greater. But despite the growing threat, the general public are less prepared than they ever have been to cope with an attack. With Trump in the White house, Putin in the Kremlin, North Korea testing ballistic missiles and the perilous state of military security, nuclear war is a real possibility.

It would kill millions (perhaps billions) of people, leave many more seriously injured, coat the planet in radioactive fallout and destroy the ecosystem. The Doomsday clock, which measures how close we are to apocalypse, has been moved from five to three minutes to midnight. Time is short – but the United Kingdom is not ready.

The reason the United Kingdom is so poorly prepared can be traced back to fairly recent times. In May 1980, the government created a series of public information films, radio broadcasts and the booklet Protect and Survive, which has now been reissued by The Imperial War museum. (The museum has said this is not



in response to the current political situation, but as part of the first major exhibition on the anti-war movement.)

Protect and Survive was widely mocked for its advice, which included painting windows with white emulsion to reflect the heat flash from a nuclear explosion, storing water in toilet cisterns, and guidance on how to bury and label the dead. In response, the BBC showed a bleak film called Threads which showed how useless the advice would have been for most city dwellers. The Campaign for Nuclear Disarmament produced a version called Protest and Survive.

The failure of Protect and Survive is the reason the United Kingdom doesn't have public information on how to prepare for a nuclear war today.

My research reveals that the Home Office repeatedly attempted to resurrect Protect and Survive throughout the 1980s. It was hoped that a new and improved public information campaign would include the use of deep nuclear shelters, make provision for vulnerable people, and promote collective planning for a nuclear attack. The Home Office even employed an advertising agency which surreptitiously attended CND meetings to keep an eye on the opposition.

The planned new version of Protect and Survive would also cover advice on preparing for a chemical or biological attack.

The Home Office's failed aim was to produce a fresh public information package, including as many as twenty new television films to be produced by 1987.

But there are three reasons why it never happened. First, other government departments, particularly the Foreign Office and the Ministry of Defense, did not want the population to be reminded that Britain was the base for a new range of US nuclear weapons. In 1982, the Home Defense committee considered that fear of embarrassing the US military would be a good reason not to issue new guidance on protection against nuclear attack. It stated in a secret memo: "In the light of experience at Greenham Common, the United States might be concerned about the further focusing of public attention on their UK installations."

Second, new psychological studies had appeared which suggested that people might not be willing to follow *any* government advice in the event of a nuclear war. A Home Office report, "Population response to war," written in 1982, decided that the

social and economic burden on the United Kingdom might be such that the country would never recover.

Faced with social collapse on such a massive scale, it was predicted that the population would simply not follow official advice. People would try and escape rather than staying at home and hoarding food, in line with government guidelines. **It was also predicted that the majority of the population would suffer from**

clinical depression after a nuclear attack and be mentally unable to follow instructions.

Finally, there was deep and vocal opposition to civil defense in the United Kingdom. The advertising agency commissioned by the Home Office considered the general public to be apathetic and fatalistic with regard to their prospects for survival. Some local authorities declared themselves "nuclear free zones" and refused to consider civil defense measures. Even though a proportion of the population would have welcomed some form of advice, the critics made it difficult to produce any information that would not be immediately rejected in the media.

Ignorance is bliss

In 1989, the Berlin Wall fell and the pressing need to create a civil defense campaign disappeared along with the Cold War. Apart from some generic information on national emergencies, it is currently almost impossible to find out what we should do in the event of a nuclear attack. In some ways, this is what the government intended even before Protect and Survive, which was originally supposed to be released only if the prospect of a nuclear war looked likely.

Indeed there are good reasons for keeping us unaware. Releasing guidance may cause anxiety and even make other countries suspicious that our preparations are a sign that we intend to strike first.

On the other hand, if the government does intend to issue information at the last minute then it is taking a huge risk as to whether it can get the advice out in time. If an accidental launch, or an unexpected first strike, occurs then there may be no time. Maybe now is the right time to buy that reprinted copy of Protect and Survive – just in case.

Protect and Survive is published to coincide with IWM's major new exhibition People Power: Fighting for Peace.

***John Preston** is Professor of Education, University of East London.*

'No one has inhaled this much plutonium': 5 staff exposed to radiation in Japan lab accident

Source: https://www.rt.com/news/391283-japan-nuclear-accident-plutonium/

June 07 – **Japanese authorities are unsure about the medical prognosis for five staffers who inhaled toxic plutonium after mishandling it at the Oarai Research and Development Center outside Tokyo.**

"As far as I can remember, no one has inhaled plutonium at this level," said Ishikawa Keiji, a security official at the Japan Atomic Energy Agency (JAEA) which oversees the lab, cited by the Jiji Press news agency.

The accident occurred at 11:15am on Tuesday in the analysis room of the facility dedicated to researching improved nuclear fuel for its fast reactors.

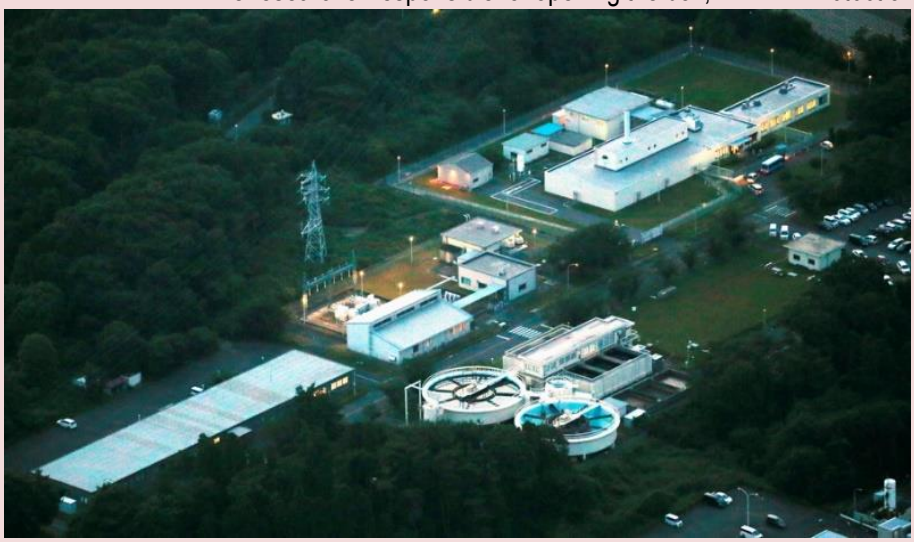
One of the five men opened a metallic cylinder where the fuel, a mixture of uranium and plutonium, is stored before and after experiments. In the process, the double plastic wrapping inside which the radioactive material is kept ripped, and the toxic substance burst into the air.

Shunichi Tanaka, chairman of the Nuclear Regulation Authority (NRA), which has frequently criticized the JAEA for the conditions at its facilities, said *"workplace complacency"* was possibly to blame.

The NRA said the workers had never experienced a similar plastic rip before,

and as a result, did not feel the need to complete their research in a tightly sealed environment.

The researcher responsible for opening the box,



described as a man in his 50s, had 22,000 becquerels of plutonium-239 detected in his lungs, and the other four between 2,200 and 14,000 becquerels.

Officials said the five staff have not yet complained of health problems with one assuring that *"the amount is not enough to cause acute radiation damage,"* according to the Japanese newspaper The Asahi Shimbun.

The longer-term predictions were less definitive, however.

"Detection of 22,000 becquerels is a situation that cannot be easily brushed aside. It is no small amount, although it may not be life-threatening," said Nobuhiko Ban, an NRA radiological protection specialist, quoted by The Asahi Shimbun.

The five have been injected with a substance that speeds up the discharge of radioactive materials and remain under observation at the National Institutes for Quantum and Radiological Science and Technology.

The NRA has previously said that JEAA was *"unfit"* to operate an accident-plagued prototype reactor at Monju and has also faced accusations of poor handling of radioactive materials at another site.

But a use for Japan's large plutonium stockpile must be found, and there are currently plans for utilizing MOX fuel – a mixture of plutonium and uranium, such as that involved in the latest accident – to power conventional reactors instead of the low-enriched uranium that they were designed for.

Dozens of new cracks discovered at Belgian nuclear reactors

Source: https://www.rt.com/news/391826-belgium-nuclear-reactor-cracks/

June 11 – **The latest ultrasonic inspections have detected a substantial number of new micro cracks in nuclear reactors at the Tihange and Doel power plants in Belgium** since the last study conducted three years ago, Belgian and German media report.

At least 70 additional cracks were uncovered at

the Tihange 2 nuclear reactor during an ultrasonic inspection in April of this year, Belga news agency reports. Some 300 new flaws have also allegedly been discovered at the Doel 3 reactor tank during a check last November, according to tagesschau.de.

Belgian Interior Minister, Jan Jambon, confirmed the micro fissures at Tihange 2 following a parliamentary inquiry posed by Green Group leader Jean-Marc Nollet, DW reports. The reported new cracks at Doel 3 have not yet been confirmed.

The cracks do not pose any danger to operations at the nuclear plants, says operator Engie-Electrabel, which carried out the inspections under instructions from the Belgian Atomic Regulatory Authority (FANC).

The operator said the new flaws were discovered due to a *"different positioning of the ultrasound device."* Engie-Electrabel maintains that as long as cracks do not expand, they do not pose a danger to the reactor's operations.

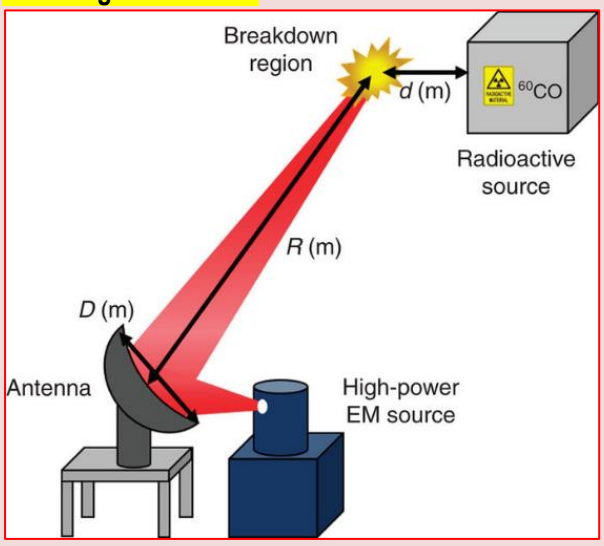
Branding Engie-Electrabel *"irresponsible,"* environmentalist group, Nucléaire Stop, has criticized the

operator for still running Tihange 2 reactor despite a 2.22 percent increase in faults.
In February 2015, FANC said 3,149 cracks had been found at Tihange, while 13,047 were discovered at Doel. The operator must now submit additional analyzes of the situation by September.
Tihange lies only 60 kilometers (about 37 miles) from the German border, while Doel is 150 kilometers away, near Antwerp. Germans living in the area close to this border have been exerting pressure on the government to force Belgium to shut down the aging reactors.
Both of the reactors have experienced leaks and cracks for some time now. Doel 3 has a capacity of 1,006 megawatts, while Tihange 2 a capacity of 1,008 megawatts. The reactors are almost 35-years-old but are still generating about 14 percent of the nation's power capacity.

Remote detection of hazardous radioactive substances

Source: http://www.homelandsecuritynewswire.com/dr20170612-remote-detection-of-hazardous-radioactive-substances

June 12 – **A recent study, affiliated with UNIST has introduced a method for the remote detection of hazardous radioactive substances. With the help of this newly developed detection device, the detection of various types of radioactive materials can be done from a remote distance.**
UNIST says that in their study, published in the May issue of the prestigious journal, *Nature Communications*, Professor Eunmi Choi of Natural Science and her team demonstrated a method with higher sensitivity that uses high-power pulsed electromagnetic-waves to detect a radioactive source.
A substance is said to be radioactive if it contains atoms with unstable nuclei and gives out nuclear radiation in the form of alpha particles, beta particles or gamma rays. Uranium-235 (U-235) is an isotope of uranium widely used for nuclear power generation and, like all other radioactive isotopes used in medicine, it has been also employed for diagnosis and treatment of diseased organs and tumors. They are essential to mankind, but can have fatal consequences if it is accidentally leaked or used as a weapon.
Remote detection of radioactive materials is impossible when the measurement location is far from its source. Indeed, a typical radiation detectors, like **Geiger-Muller counters** have technical limitations in the remote detection of sources. For instance, they **can detect 1 milli Curie (mCi) of Cobalt-60 (60Co) at a maximum distance of 3.5 meters, but are inefficient at measuring lower levels of radioactivity or at longer distances.**



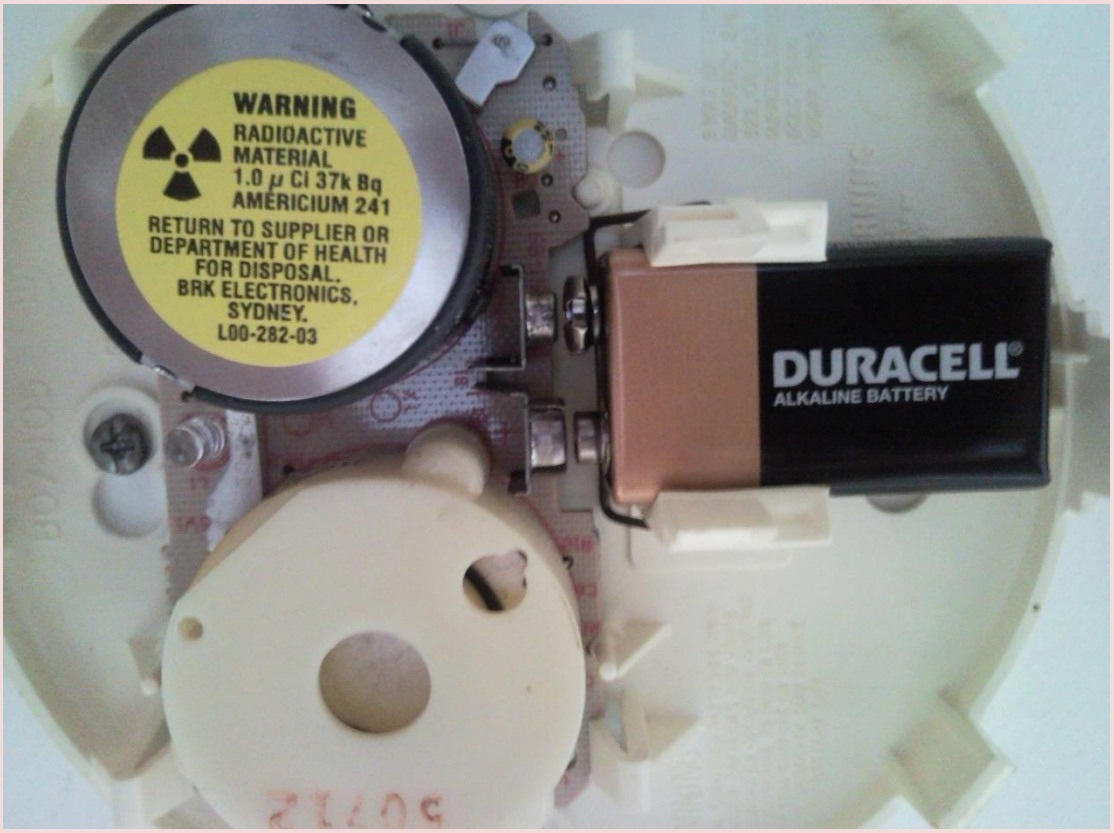
In the study, Professor Choi and her research team described the experimental demonstration of real-time radioactive material detection **using a high-power pulsed millimeter-wave source**. They demonstrated the **detection of 0.5 μg of cobalt-60 from 120 cm away, the maximum distance allowed by the laboratory setup.**
"With the existing technologies, remote detection of radioactive materials is impossible when the measurement location is far from the radioactive source," says Dongsung Kim (Combined M.S./Ph.D. student of Physics), the first author of the study. "The detection sensitivity has been increased to 4,800 times, compared to the conventional theoretical sensitivity, enabling the detection of very small amounts of radiation."
"Depending on the equipment used, this method could scale to detect radioactivity at distances of at least tens of kilometers and possibly as far as 100 km," says Professor Choi.

— Read more in Dongsung Kim et al., "Remote detection of radioactive material using high-power pulsed electromagnetic radiation," Nature Communications 8, Article number: 15394 (9 May 2017).

Dirty letters

▶ From: 2017 EU Terrorism Situation & Trend Report (Te-Sat) – p.16
Source: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017

In November 2016, several Slovak institutions including the Ministry of Justice, district courts and a regional police office, received suspicious envelopes containing anonymous letters. The letters expressed dissatisfaction with the judicial system and mentioned a lost court trial.
One letter referred to radioactive contamination and incidents in 2015 and 2016 when employees of various judicial institutions were exposed to radioactive material emitting **alpha-particles.** Further



laboratory expertise confirmed the presence of **small amounts of radioactive Americium-241 in the envelopes** [**half life:** 432.2 yrs]. The case was investigated by the Slovak authorities as an act of terrorism. This incident demonstrated that certain CBRN materials that are commonly used in various civilian applications (i.e., fire detectors – see photo above), in particular radioactive substances, can be acquired by criminals or terrorists due to inadequate security measures.

Forget North Korea: Why the World Should Fear Pakistan's Nukes

By Kyle Mizokami
Source: http://nationalinterest.org/blog/the-buzz/forget-north-korea-why-the-world-should-fear-pakistans-nukes-21166?page=show

June 15 – **Pakistan is clearly developing a robust nuclear capability that can not only deter but fight a nuclear war.** It is also dealing with internal security issues that could threaten the integrity of its nuclear arsenal. Pakistan and India are clearly in the midst of a nuclear arms race that could, in relative terms, lead to absurdly high nuclear stockpiles reminiscent of the Cold War. It is clear that an arms-control agreement for the subcontinent is desperately needed.

Sandwiched between Iran, China, India and Afghanistan, Pakistan lives in a complicated neighborhood

with a variety of security issues. One of the nine known states known to have nuclear weapons, Pakistan's nuclear arsenal and doctrine are continually evolving to match perceived threats. A nuclear power for decades, Pakistan is now attempting to construct a nuclear triad of its own, making its nuclear arsenal resilient and capable of devastating retaliatory strikes.

Pakistan's nuclear program goes back to the 1950s, during the early days of its rivalry with India.

President Zulfikar Ali Bhutto famously said in 1965, **"If India builds the bomb, we will eat grass or leaves, even go hungry, but we will get one of our own."**

The program became a higher priority after the country's 1971 defeat at the hands of India, which caused East Pakistan to break away and become Bangladesh. Experts believe the humiliating loss of territory, much more than reports that India was pursuing nuclear weapons, accelerated the Pakistani nuclear program. India tested its first bomb, codenamed "Smiling Buddha," in May 1974, putting the subcontinent on the road to nuclearization.

Pakistan began the process of accumulating the necessary fuel for nuclear weapons, enriched uranium and plutonium. The country was particularly helped by one A. Q. Khan, a metallurgist working in the West who returned to his home country in 1975 with centrifuge designs and business contacts necessary to begin the enrichment process. Pakistan's program was assisted by European countries and a clandestine equipment-acquisition program designed to do an end run on nonproliferation efforts. Outside countries eventually dropped out as the true purpose of the program became clear, but the clandestine effort continued.

Exactly when Pakistan had completed its first nuclear device is murky. Former president Benazir Bhutto, Zulfikar Bhutto's dau ghter, claimed that her father told her the first device was ready by 1977. A member of the Pakistan Atomic Energy Commission said design of the bomb was completed in 1978 and the bomb was "cold tested"—stopping short of an actual explosion—in 1983.

Benazir Bhutto later claimed that Pakistan's bombs were stored disassembled until 1998, when India tested six bombs in a span of three days. Nearly three weeks later, Pakistan conducted a similar rapid-fire testing schedule, setting off five bombs in a single day and a sixth bomb three days later. The first device, estimated at twenty-five to thirty kilotons, may have been a boosted uranium device. The second was estimated at twelve kilotons, and the next three as sub-kiloton devices.

The sixth and final device appears to have also been a twelve-kiloton bomb that was detonated at a different testing range; a U.S. Air Force "Constant Phoenix" nuclear-detection aircraft reportedly detected plutonium afterward. Since Pakistan had been working on a uranium bomb and North Korea—which shared or purchased research with Pakistan through the A. Q. Khan network—had been working on a uranium bomb, some outside observers concluded the sixth test was actually a North Korean test, detonated elsewhere to conceal North Korea's involvement although. There is no consensus on this conclusion.

Experts believe Pakistan's nuclear stockpile is steadily growing. In 1998, the stockpile was estimated at five to twenty-five devices, depending on how much enriched uranium each bomb required. Today Pakistan is estimated to have an arsenal of 110 to 130 nuclear bombs. In 2015 the Carnegie Endowment for International Peace and the Stimson Center estimated Pakistan's bomb-making capability at twenty devices annually, which on top of the existing stockpile meant Pakistan could quickly become the third-largest nuclear power in the world. Other observers, however, believe Pakistan

can only develop another forty to fifty warheads in the near future.

Pakistani nuclear weapons are under control of the military's Strategic Plans Division, and are primarily stored in Punjab Province, far from the northwest frontier and the Taliban. Ten thousand Pakistani troops and intelligence personnel from the SPD guard the weapons. Pakistan claims that the weapons are only armed by the appropriate code at the last moment, preventing a "rogue nuke" scenario.

Pakistani nuclear doctrine appears to be to deter what it considers an economically, politically and militarily stronger India. The nuclear standoff is exacerbated by the traditional animosity between the two countries, the several wars the two countries have fought, and events such as the 2008 terrorist attack on Mumbai, which were directed by Pakistan. Unlike neighboring India and China, Pakistan does not have a "no first use" doctrine, and reserves the right to use nuclear weapons, particularly low-yield tactical nuclear weapons, to offset India's advantage in conventional forces.

Pakistan currently has a nuclear "triad" of nuclear delivery systems based on land, in the air and at sea. Islamabad is believed to have modified American-built F-16A fighters and possibly French-made Mirage fighters to deliver nuclear bombs by 1995. Since the fighters would have to penetrate India's air defense network to deliver their payloads against cities and other targets, Pakistani aircraft would likely be deliver tactical nuclear weapons against battlefield targets.

Land-based delivery systems are in the form of missiles, with many designs based on or influenced by Chinese and North Korean designs. The Hatf series of mobile missiles includes the solid-fueled Hatf-III (180 miles), solid-fueled Hatf-IV (466 miles) and liquid-fueled Hatf V, (766 miles). The CSIS Missile Threat Initiative believes that as of 2014, Hatf VI (1242 miles) is likely in service. Pakistan is also developing a Shaheen III intermediate-range missile capable of striking targets out to 1708 miles, in order to strike the Nicobar and Andaman Islands.

The sea component of Pakistan's nuclear force consists of the Babur class of cruise missiles. The latest version, Babur-2, looks like most modern cruise missiles, with a bullet-like shape, a cluster of four tiny tail wings and two stubby main wings, all powered by a turbofan or turbojet engine. The cruise missile has a range of 434 miles. Instead of GPS guidance, which could be disabled regionally by the U.S. government, Babur-2 uses older Terrain Contour Matching (TERCOM) and Digital Scene Matching and Area Co-relation (DSMAC) navigation technology. Babur-2 is deployed on both land and at sea on ships, where they would be more difficult to neutralize. **A submarine-launched version, Babur-3, was tested in January and would be the most survivable of all Pakistani nuclear delivery systems.**

Pakistan is clearly developing a robust nuclear capability that can not only deter but fight a nuclear war. It is also dealing with internal security issues that could threaten the integrity of its nuclear arsenal. Pakistan and India are clearly in the midst of a nuclear arms race that could, in relative terms, lead to absurdly high nuclear stockpiles reminiscent of the Cold War.

It is clear that an arms-control agreement for the subcontinent is desperately needed.

Kyle Mizokami *is a defense and national-security writer based in San Francisco who has appeared in the Diplomat, Foreign Policy, War is Boring* and the *Daily Beast*. In 2009, he cofounded the defense and security blog *Japan Security Watch*.

"Dirty Bomb" Threat on Vessel Investigated – What is the Significance?

Source: http://i-hls.com/archives/77102

June 15 – The Port of Charleston, South Carolina, has been evacuated early June 15th as US federal authorities investigate a reported threat on a container ship that had **arrived there from New York**, according to reports. The port's Wando Welch terminal was cleared out as the Coast Guard and FBI investigated the possible threat described as an unconfirmed report of a "dirty bomb" on the ship, according to South Carolina's WCSC-TV.

The commander of the local Coast Guard sector told Charleston's WCIV that the unconfirmed claim was made by a YouTube "conspiracy theorist" but they were investigating out of an abundance of caution.
The vessel was reported as the **Maersk Memphis** [photo below], which docked around 8:30 p.m. Wednesday and traveled from New York.

A dirty bomb or radiological dispersal device (RDD) is a radiological weapon that combines radioactive material with conventional explosives. The purpose of the weapon is to contaminate the area around the dispersal agent/conventional explosion with radioactive material, serving primarily as an area denial device against civilians.
It is however not to be confused with a nuclear explosion, such as a fission bomb, which by releasing nuclear energy produces blast effects far in excess of what is achievable by the use of conventional explosives.
Though an RDD would be designed to disperse radioactive material over a large area, a bomb that uses conventional explosives and produces a blast wave would be far more lethal to people than the hazard posed by radioactive material that may be mixed with the explosive.

Possible correlation found between TMI meltdown and thyroid cancers

Source: http://www.homelandsecuritynewswire.com/dr20170619-possible-correlation-found-between-tmi-meltdown-and-thyroid-cancers

June 19 – Penn State College of Medicine researchers have shown, for the first time, **a possible correlation between the partial meltdown of the Three Mile Island Nuclear Generating Station and thyroid cancers in the counties surrounding the plant.**
Three Mile Island (TMI), located near Harrisburg, Pennsylvania, had a partial meltdown accident on 28 March 1979. During the accident, radiation was released into the environment, which the United States Nuclear Regulatory Commission said was in small amounts with no detectable health effects.

Looking at tumor samples from people verified to have lived in the areas around TMI at the time of the accident, remained in the area and subsequently developed thyroid cancer, researchers observed a shift in cases to cancer mutations consistent with radiation exposure, from those consistent with random causes.

Penn State says that in this retrospective cohort study — meaning the patients in the study already had thyroid cancer and were known to have been exposed to the TMI accident — lead researcher David Goldenberg, professor of surgery, and colleagues identified 44 patients who were treated at the Penn State Milton S. Hershey Medical Center for the most common type of thyroid cancer — papillary thyroid cancer — between 1974 and 2014. The patients were then divided into two groups: at-risk and control groups.

Patients in the at-risk group were those who developed cancer between 1984 and 1996, consistent with known latency periods of radiation-induced thyroid cancer, and who lived in at-risk geographical areas — based on reported weather patterns — at the time of the accident.

"This definition was designed to allow us to identify relatively acute effects of radiation exposure from the accident," said Goldenberg.

Patients who developed cancer outside of the expected latency period were placed in the control group.

Researchers searched through all thyroid cancer tumor samples in the hospital's possession from the study period for patients who lived in at-risk regions Dauphin, York, eastern Cumberland, Lancaster and western Lebanon counties. They used genealogical software to verify that the patient was in an at-risk area during the accident, remained until cancer developed and was treated at the Medical Center. The tumor samples of those patients who were positively linked to the TMI accident area were then processed through the Penn State Institute for Personalized Medicine to determine genetic makeup of the cancer.

While most thyroid cancers are sporadic, meaning they happen without clear reasons, exposure to radiation has been shown to change the molecular makeup of the cancer, according to the researchers.

The researchers observed an increase in the genetic mutation caused by exposure to low-dose radiation in the at-risk group and a decrease in the incidence of sporadic thyroid cancer, identified by a specific genetic mutation known as BRAF. The BRAF mutation is typically not present in the radiation-induced types of thyroid cancer.

The study, which appeared in ay 29 supplement to the journal *Laryngoscope*, indicates that these observations are consistent with other radiation-exposed populations.

In the control group, 83 percent of patients had the BRAF mutation. The BRAF mutation was found in only 53 percent of patients in the at-risk group. In the at-risk group, there was also a rise in other molecular markers seen in radiation-induced thyroid cancer, the researchers added.

"While no single marker can determine whether an individual tumor is radiation-induced, these data support the possibility that radiation released from TMI altered the molecular profile of thyroid cancers in the population surrounding the plant," Goldenberg said.

A limitation of this study is the small sample size, limited to tumor samples from patients treated for thyroid cancer at Penn State Health Milton S. Hershey Medical Center. The next step in the research is a study with a larger number of patients from other regional hospitals to determine if the correlation continues in a larger sample.

"All patients were screened extensively to ensure that they lived in the vicinity of TMI from the date of the accident until they developed thyroid cancer," Goldenberg said. "We used an extensive vetting process to ensure that patients included in the study were present in at-risk counties at the time of the accident and to confirm, to the greatest extent possible, that patients resided in affected areas for their entire lives. Our study represents a static population, which increased our ability to detect radiation-induced cancers."

Past studies about thyroid cancer and TMI have showed variable results, mainly because they were demographic studies that looked at the entire population and not just those who met the criteria of the current study.

"Much of the variability associated with these studies is likely due to the relatively small size of the population surrounding the TMI plant relative to the large population required to detect statistically significant increases in cancer incidence following low-level radiation, combined with a high degree of mobility in the local population," Goldenberg said.

— Read more in David Golcenberg et al., "Altered molecular profile in thyroid cancers from patients affected by the Three Mile Island nuclear accident," Laryngoscope (29 May 2017).

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

EXPLOSIVE NEWS

Why banning laptops from airplane cabins doesn't make sense

By Cassandra Burke Robertson and Irina D. Manta

Source: http://www.homelandsecuritynewswire.com/dr20170522-why-banning-laptops-from-airplane-cabins-doesn-t-make-sense

May 22 – Recent reports suggest that terrorists can now create bombs so thin that they cannot be detected by the current X-ray screening that our carry-on bags undergo.

In an effort to protect against such threats, the U.S is considering banning laptops and other large electronic devices in the passenger cabins of airplanes flying between Europe and the United States. This would extend a ban already in place on flights from eight Middle Eastern countries.

Given the significant disruption such a policy would cause tens of thousands of passengers a day, a logical question any economist might ask is: Is it worth it?

It is tempting to think that any level of cost and inconvenience is sensible if it reduces the risk of an attack even a little. But risks, inherent in flying and even driving, can never be avoided entirely. So when weighing policies that are designed to make us safer, it is important to consider both their costs and potential effectiveness.

Unfortunately, whether the benefits justify the costs is too often not the yardstick used by officials determining whether to pursue these types of policies. Instead, as law professors who have researched how the government's travel policies affect civil liberties, we have found that it is more likely that political considerations motivate the adoption of restrictive policies, which in the end actually do little to protect citizens' security.

Expanding a ban

The current laptop policy regarding some flights from the Middle East was put in place in March apparently as a result of intelligence that ISIS militants were training to get laptop bombs past security screeners and onto planes. The U.K. adopted a similar rule.

The Department of Homeland Security wants to extend that ban to transatlantic flights. This would cause major disruption and "logistical chaos." Approximately 65 million people a year fly between Europe and the United States.

Business travelers are concerned about the loss of productivity and the risk that a checked laptop with sensitive information could be damaged, stolen or subjected to intrusive search. Families worry about traveling without electronic distractions to soothe tired and uncomfortable children. Airlines expect a loss of business as people opt out of transatlantic travel altogether.

Past policies such as limiting the liquids that can be carried on and requiring passengers to remove shoes are a case in point. They have increased burdens on both travelers – who must pay to check baggage and face added inconvenience – and taxpayers – who bear the costs of every policy change – while likely doing little to nothing to improve security.

Benefits and costs

Regulators throughout the government typically must rely on a cost-benefit analysis to determine levels of acceptable risk, weighing the potential safety gain of a new policy against its costs and added risks.

But when dealing with a fear of terrorism, it is common to find policies that are not cost effective. And if we subjected the laptop bans (the original and expansion) to a cost-benefit analysis, they would likely fail. The costs are high, the potential security gains are small, and the policy adds hazards of its own.

To make its case, the government seems to be relying on several purported benefits of stowing laptops in the luggage hold. First, checked bags undergo additional screening for the presence of explosives. Second, it is possible that luggage in the cargo area could provide some insulation from an explosion. Finally, bombs placed in the cargo area require a sophisticated timing device, unlike simpler explosives that could be set off manually.

But these benefits appear dubious as support for a laptop ban. Carry-on luggage could go through expanded screening, for example, while the notion that checked luggage might

make an explosion more survivable is speculative – and such gains might in any case be offset by the dangerous greater vibration found in cargo cabin. Lithium batteries have, after all, been forbidden from the cargo compartment for a reason – and must instead be carried on – to avoid the risk of fire.

And of course, this does little to protect against the risk of an explosive device in the cargo cabin. It just moves the risk to an isolated area of the plane.

Moving the devices to the hold could actually make such devices harder to detect if they slip past airport screening. The exploding lithium batteries in Samsung devices, for example, show how even ordinary fire risks can be greater when passengers are not there to notice a smoking battery in a bag in the overhead compartment.

Similarly, the presence of observant passengers can help thwart terrorist activity when it does occur, as happened with the underwear bomber.

One should keep in mind that one of the greatest airline tragedies of all times, the attack on Pan Am flight 103 that exploded over Lockerbie and claimed 270 lives, was caused by a bomb that went off in a suitcase in the cargo hold.

On the economic side, the financial costs of the policy change would likely be very high. Based on statistics from the U.S. Department of Commerce, travel industry professionals estimate that the cost of lost productivity alone for business travelers unable to work on flights between the U.S. and Europe is estimated to be as great as $500 million a year.

The potential loss of tourism revenue may be even greater, as families avoid vacationing in the United States and business travelers choose to meet by teleconference instead of in person.

Questionable politics

So if the laptop ban would be ineffective – or worse yet, even make airline travel less safe – and be very costly, why would the government consider it?

The answer is likely politics. And that is because people overestimate the likelihood of being harmed by a terrorist attack, which lends extreme actions like the laptop ban public support, while they underestimate the risks of more ordinary occurrences like car accidents or defective batteries.

From 1975 to 2015, fewer than 84 Americans a year died due to terrorism, and that includes the attacks on 9/11. Meanwhile, in 2015 alone a total of 38,300 people died in traffic-related accidents in the U.S. And lithium batteries have been blamed for dozens of aircraft fires and may have been what brought down Malaysia Airlines Flight 370, which disappeared in 2014 with more than 200 passengers and crew.

At the same time, officials on whose watch an attack or other disaster occurs receive disproportionate blame, something that does not carry over to more ordinary risks. People fear terror attacks more than the common threats that are actually more likely to cause them harm. Politicians may respond to their voters' concerns, and may even share the same cognitive biases.

As a result, government decision makers have an incentive to overvalue measures taken to prevent terror attacks, even at the expense of increasing more ordinary – yet more likely – safety risks.

While there may not be much we can do about Americans' misconceptions about the risk of terrorism, public policy on an issue as important as airline safety should not blindly follow them.

Cassandra Burke Robertson *is Professor of Law and Director of the Center for Professional Ethics, Case Western Reserve University.*
Irina D. Manta *is Professor of Law and Director of the Center for Intellectual Property Law, Hofstra University.*

Hospital Bomb In Thai Capital, Bangkok, Wounds 24

Source: http://m.ndtv.com/world-news/hospital-bomb-in-thai-capital-bangkok-wounds-24-police-1696661?pfrom=home-world

May 22 – **A bomb blast at a hospital in the Thai capital, Bangkok, wounded 24 people on Monday, on the third anniversary of a 2014 military coup.** There was no claim of responsibility for the blast at the Phramongkutklao Hospital, which is popular with retired military officers. "It was a bomb. We found the pieces that were used to make the bomb,"

Kamthorn Aucharoen, commander of the police's explosive ordnance team, told Reuters. "Right now, authorities are checking out closed circuit cameras." Government spokesman Sansern Kaewkamnerd said 24 people had been wounded. Most of the wounded were hit by flying glass, the military's national security unit said.

Suspicion is likely to focus either on political dissidents opposed to military rule or Muslim separatists based in the south of the predominately Buddhist country.

Soldiers cordoned off the hospital's entrance, a Reuters reporter at the scene said.

Deputy national police chief General Srivara Rangsibrahmanakul said the bomb had been hidden in a container by the entrance of a pharmacy.

Monday is the anniversary of a May 22, 2014, military coup that toppled a democratically elected government and ended months of unrest, including sometimes deadly street demonstrations.

Since the coup, the junta, known as the National Council for Peace and Order, has clamped down on dissent and ramped up prosecutions under sedition and royal defamation laws.

Blasts in South

The military has always played a prominent role in Thai life but since the coup it has become embedded in society with military men more entrenched than under previous governments.

The military government has acknowledged it wants to weaken political parties and maintain permanent influence over elected governments, partly through a new constitution approved by the king last month. An election is due by the end of next year.

The blast comes weeks after a car bomb at a shopping center in the province of Pattani, near Thailand's border with Malaysia, which wounded 61 people, and which authorities blamed on the Muslim insurgents.

The far south of Thailand, which includes Pattani, Yala and Narathiwat provinces, is home to a long-running separatist insurgency.

Earlier on Monday, a bomb went off in Yala, one of the Muslim-majority provinces in the restive south, wounding military officers.

Attacks by the Muslim rebels have largely, though not always, been confined to their southern heartland.

On May 15, a small bomb went off near the National Theater in Bangkok's old quarter, wounding two people. It was not clear who was behind the bomb.
New York-based Human Rights Watch said it condemned the hospital attack as "a cruel and inhumane action which grossly violates human rights", Sunai Phasuk, the group's senior Thailand researcher said on Twitter.

Former PM Lucas Papademos injured in car explosion

Lucas Papademos, a former central bank chief, admitted to hospital in Athens after being targeted by explosive device.

Source: http://www.aljazeera.com/news/2017/05/pm-lucas-papademos-injured-explosion-170525162952789.html

May 25 – **Lucas Papademos, Greece's former prime minister and ex-central bank chief, has been injured after an explosive device hidden in an envelope went off inside his car in the capital, Athens.**

Papademos, 69, on Thursday sustained "several superficial wounds on his chest, abdomen and thighs", but his condition is stable and his injuries are not life-threatening, according to a statement by Evangelismos Hospital.

He was taken to the hospital in central Athens, along with his driver and security officer who suffered "light superficial injuries" in the blast and were being kept in hospital for "precautionary reasons", said the statement.

Papademos, who was sitting at the back of the car, was hurt when the booby-trapped package he opened exploded. The driver and security officer were sitting in the two front seats.

There was no immediate claim of responsibility.

The attack was widely condemned by politicians from all major Greek parties, including Prime Minister Alexis Tsipras, who is in Brussels for a NATO summit.

"I unequivocally condemn the attack against Lucas Papademos. I wish a speedy recovery to him and the people who accompanied him," Tsipras wrote in a message on Twitter.

Papademos, known more as a technocrat and an economist than a politician, was catapulted to the forefront of Greece's debt crisis when he was coaxed into briefly becoming caretaker prime minister from November 2011 until elections in May 2012, fusing a fragile governing coalition between socialists and conservatives.

He has also served as vice president of the European Central Bank (ECB).

Wounded former PM transferred to ambulance

Mario Draghi, the ECB president, also condemned the attack: "We are saddened by the attack against our former colleague, Lucas Papademos, a brave public servant of Greece and Europe."

As to why Papademos may be targeted, Al Jazeera's John Psaropoulos, reporting from Athens, said "he was prime minister during a very controversial period during the Greek bailout".

"During that time, two controversial things happened: Minimum wage was lowered by 20 percent, which is an act that is still talked about in controversial terms; and Greece discounted its bonds by 75 percent, which means that most of the value of those bonds held by private entities, including pension funds, was wiped out," Psaropoulos said.

"Essentially, that bankrupted the pension funds, meaning they have been supported by the government ever since. Those two acts are considered to have been done by Papademos, who was an unelected prime minister."

Suspect packages

Greece has a history of small-scale attacks against politicians, businesses and police.

In March, police intercepted eight suspect packages at a postal sorting centre in Athens, days after letter bombs were sent to the German finance ministry and the International Monetary Fund in France's capital, Paris.

The rigged package to the IMF exploded, injuring an employee, while the one sent to Germany was detected by scanners.

A Greek group called Conspiracy of Fire Cells claimed responsibility for the first suspect package sent to Germany and intercepted on March 15

Greece remains in recession with the highest unemployment rate in Europe, and a stalled creditor review has interrupted payouts under its international bailout programme, its third since 2010.

EDITOR'S COMMENT: (Unfortunately) it takes a bombing to reveal gaps in various SOPs. In this case many were revealed. Perhaps the most prominent was to open incoming postal correspondence inside a confined space (a car). Now the system is exploring what happened but is is too late! Perhaps they should start studying the new tech advances in future IEDs [i.e. printed detonators; explosives in a chip; printed flexible batteries), and proceed in pre-emptive planning to avoid new surpises (as usual). Ah! Also a good opportunity to buy some explosives' detectors – so if you miss content in x-rays, might get a trace warning… There is also a "game" played by a "red" team against a "green" team – if you know what I mean!

After the Manchester Arena massacre...

Manchester: Saved by her iPhone

45 yo Lisa Bridgett was saved by her iPhone (while making a phone call), that stopped one of the metal bolts contained in the bomb detonated during the Manchester Arena incident. She lost a finger but she is alive.

ISIS claims first suicide attack in Somalia, kills 5

Source: http://m.timesofindia.com/world/middle-east/isis-claims-first-suicide-attack-in-somalia-kills-5/articleshow/58821717.cms

May 25 – **The Islamic State group has claimed its first suicide attack in Somalia,** which police said Wednesday killed five people at a checkpoint in the northeastern port city of Bosaso.
The group's self-styled news agency Amaq claimed the "martyrdom-seeking operation with an explosive vest" in a statement carried by the SITE Intelligence Group.
The suicide bomber detonated his explosives vest at a checkpoint late Tuesday in the **semi-autonomous** region of Puntland.
"Security forces stopped the suspect when he approached but he detonated himself leaving five people dead. One of the security officers and four civilians were killed in the blast," said local police official Mohamed Dahir Adan.

The blast occurred near a hotel often used as a meeting place for local officials, witnesses said.
"I think the bomber was trying to target the hotel but he was stopped at the checkpoint close to the hotel and he decided to detonate his explosives," said witness Awke Mohamed.
Puntland set up its own government in 1998, but, unlike neighbouring Somaliland, it has not declared full independence. The region has often come under attack by Al-Qaeda-linked Shabaab militants, and is also home to a breakaway group of fighters which declared allegiance to IS last year but has failed to gather much support so far. The militants are led by former Shabaab cleric Abdiqadir Mumin who was placed on a US terror list last August for his role at the head of IS in East Africa.

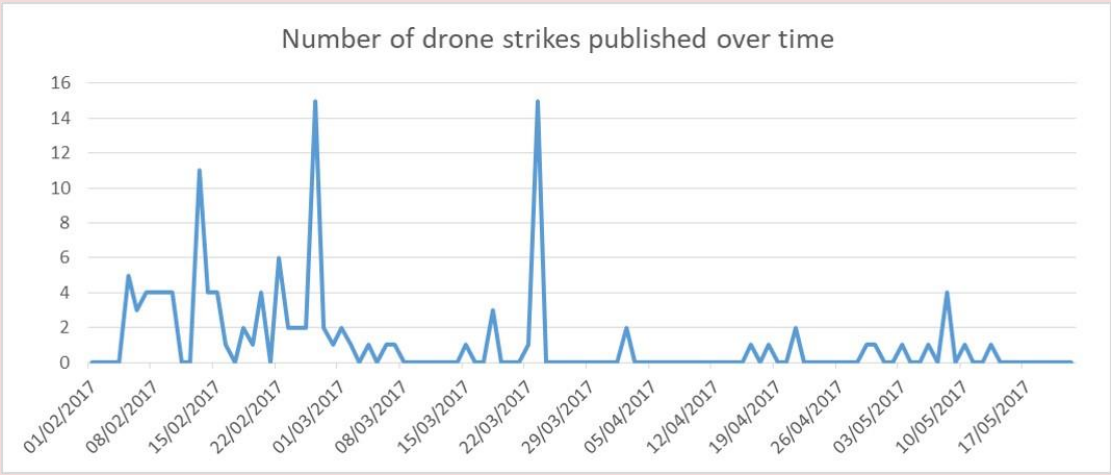
Types of Islamic State Drone Bombs and Where to Find Them

By Nick Waters
Source: https://www.bellingcat.com/news/mena/2017/05/24/types-islamic-state-drone-bombs-find/

May 24 – The proliferation of armed, commercially sourced drones has become a fact of the current conflict in Iraq and Syria. Jund Al Aqsa, Hezbollah, so called Islamic State (IS) and Iraqi Government forces have all used commercial drones which have been modified to carry either improvised bombs, or in the case of Hezbollah, sub-munitions from a cluster bomb. The types of munitions dropped by drones is surprisingly varied, and different kinds of drone bombs appear in different theatres of conflict, no doubt influenced by a wide range of different factors from the people who make them, to the materials available.
The Drone Strike Database has logged images of 121 strikes using media released by IS up to 23 May 17, and includes a spreadsheet showing the earliest identified date the strike was published, as well as

the location, presumed target and kind of munition used in each strike. This data has been input into a Silk, allowing readers to explore the data for themselves. The Silk includes an interactive map where we can see details of how particular types of IS drone bombs can be found in distinct geographical locations. Please note that Silk is no longer supported and its user interface can take a while to understand, but once it has been mastered it can provide an excellent place to view data.

Plastic 6-fin tail



This article uses the data set to analyse and log the different kinds of drone bombs that IS has used, where they have been used, and on what targets. By its nature, this data-set uses information that comes from IS, and so it must be understood that this is not a complete representation of IS drone operations. Rather it is a subset of their drone operations presenting strikes they wished to be seen. It should also be noted that the location of these drone strikes is rough, and accurate only at provincial level, except where exact co-ordinates have been specified. Strikes which contained no information about their location have been geo-tagged to a location in the Mediterranean Sea to keep them within the frame of the map, while making it obvious that their location is unknown.

▶▶ Read the rest of this very interesting article at source's URL.

Nick Waters *is an ex-British Army officer and open source analyst. He has a special interest in the conflicts in Afghanistan and Ukraine, as well as intelligence, security and international development.*

ISIS in plot to blow up British ports by planting bombs on fuel tankers

Source: http://www.express.co.uk/news/world/807723/ISIS-British-ports-plot-blow-bombs-fuel-tankers-Kent-Wales-Daesh-attack-UK-Royal-Navy

May 22 – Intelligence reports revealed plots to attach explosives to the side of vessels carrying millions of tons of liquid natural gas from the Middle East to Britain, according to the Mail on Sunday.

Secret searches have taken place in docks around the world over the last two years in a effort to prevent a horrific explosion which would have a disastrous environmental impact and could potentially cause catastrophic loss of life.
Royal Navy specialists alongside the highly trained Special Boat Service (SBS) are currently conducting the covert checks to fuel-carrying tankers, which unload at terminals on the Isle of Grain in Kent and at Milford Haven in Wales.
Operations were launched amid growing threats from Al Qaeda or the Islamic State (ISIS) group.
A senior Naval source told the MoS there was a possibility terrorists could plant mines on ships inside UK waters.
The source said: "The threat against gas tankers emerged a couple years ago and we have been training to counter it ever since. The concern is that tankers could be sailed into UK waters and destroyed either with mines or improvised explosive devices (IEDs).
"It is entirely possible a major incident could result in fuel shortages in the UK and this would be disastrous economically."

A potential plot could involve a limpet mine (photo) - an IED which can be attached to a ship's hull.

Huge bomb in sewage tanker kills at least 80, wounds hundreds in Afghan capital

Source: http://www.reuters.com/article/us-afghanistan-blast-idUSKBN18R0DT

May 31 – A powerful bomb hidden in a sewage tanker exploded in the morning rush hour in the centre of the Afghan capital on Wednesday, police said, killing at least 80 people, wounding hundreds and damaging embassy buildings.

The victims appeared mainly to have been Afghan civilians.

The bomb, one of the deadliest in Kabul and coming at the start of the holy month of Ramadan, exploded

close to the fortified entrance to the German embassy, killing a security guard and wounding some staff, German Foreign Minister Sigmar Gabriel said on Twitter.

“Such attacks do not change our resolve in continuing to support the Afghan government in the stabilization of the country," he said.

Basir Mujahid, a spokesman for city police, said the explosives were hidden in a sewage tanker. He suggested that the German embassy might not have been the target of the blast, which sent clouds of black smoke into the sky near the presidential palace.

"There are several other important compounds and offices near there too," he told Reuters.

The blast, which shattered windows and blew doors off their hinges in houses hundreds of metres away, was unusually strong.

The Taliban, seeking to reimpose Islamic rule after their 2001 ouster by U.S.-led forces, denied responsibility and said they condemned attacks that have no legitimate target and killed civilians.

Islamic State, the other main militant group active in Afghanistan, has carried out high profile attacks in Kabul, including an attack on a military hospital in March that killed more than 50 people.

The NATO-led Resolute Support (RS) mission in Kabul said Afghan security forces prevented the vehicle carrying the bomb from entering the heavily protected Green Zone that houses many foreign embassies as well as its headquarters, also suggesting it may not have reached its intended target.

A public health official said at least 80 people had been killed and more than 350 wounded.

Germany cancelled a planned flight deporting migrants to Afghanistan after the blast, its ARD broadcaster said, citing the interior minister. Germany began carrying out group deportations of Afghans in December, seeking to show it is tackling the high number of migrants by getting rid of those who do not qualify as refugees.

The French, Turkish and Chinese embassies were among those damaged, the three countries said, adding there were no immediate signs of injuries among their diplomats. The BBC said one of its drivers, an Afghan, was killed driving journalists to work. Four journalists were wounded and treated in hospital.

Video shot at the scene showed burning debris, crumbled walls and buildings, and destroyed cars, many with dead or injured people inside.

"Felt like an earthquake"

At the Wazir Akbar Khan hospital a few blocks away, there were scenes of chaos as ambulances brought in wounded and frantic relatives scanned casualty lists and questioned hospital staff for news.

"It felt like an earthquake," said 21-year-old Mohammad Hassan, describing the moment the blast struck the bank where he was working. His head wound had been bandaged but blood still soaked his white dress shirt.

Another lightly wounded victim, Nabib Ahmad, 27, said there was widespread destruction and confusion. "I couldn't think clearly, there was a mess everywhere," he said.

Frenzy erupted out outside the hospital as ambulances and police trucks began bringing in the bodies of those killed. Some bodies were burned or destroyed beyond recognition.

India and Pakistan condemned the blast.

"India stands with Afghanistan in fighting all types of terrorism. Forces supporting terrorism need to be defeated," Indian Prime Minister Narendra Modi said in a tweet. India said its embassy staff were safe.

Wednesday's attack provided another clear demonstration that Ramadan, which began at the weekend, would provide little respite from the violence across Afghanistan.

The Taliban have been stepping up their push to defeat the U.S.-backed government. Since most international troops withdrew at the end of 2014, the Taliban have gained ground and now control or contest about 40 percent of the country, according to U.S. estimates, though President Ashraf Ghani's government holds all provincial centres.

U.S. President Donald Trump is due to decide soon on a recommendation to send 3,000 to 5,000 more troops to bolster the small NATO training force and U.S. counter-terrorism mission now totalling just over 10,000.

The commander of U.S. forces in Afghanistan, General John Nicholson, told a congressional hearing this year that he needed several thousand more troops to help Afghan forces break a "stalemate" with the Taliban.

Portable X-Ray Security Detection System

Source:

May 27 – Airports, central railway stations, and other large perimeters are well equipped with X-Ray screening systems for the detection of explosives or suspicious objects. **But what about screening missions in outdoor environments such as battlefields, border posts, energy installations, etc.?**

A series of portable flat-panel digital x-ray inspection systems offers an effective detection solution for sectors such as security, nondestructive testing, science, and more.

The lightweight X-ray inspection systems, developed and manufactured by the Israeli company **NOVO DR**, offer high image quality, portability, efficient user experience and field work optimization.

Every system includes at the minimum a detector, tablet and software, and an X-ray source.

The light and easy to carry complete set provides over 16 hours of continuous operation using internal batteries.

The fully ruggedized systems for security applications provide a complete solution for grabbing x-ray images in the most extreme and demanding environments, using the ultra-thin detectors.

Adar Yiron, NOVO DR's EVP Sales and Marketing, told iHLS that the systems ruggedness and their compatibility to the most extreme environments and the fact that they can be carried by the soldiers guarantee that they will function at the right moment.

The light weight of the systems results from the use of the lightest camera sensors in the market. This feature makes the systems suitable for the requirements of the special units, as they can not carry additional weight durin a mission.

Yiron adds that the company has pioneered this market with the development of a touch screen software, that is suitable for operation in harsh environments, e.g. during a sandstorm in the desert.

The user interface guarantees easy and rapid operation. In addition to the capability of optimizing images independently, the system offers also an automatic optimization tool called Genie, which supplies the highest quality image with only one touch.

For quick sharing and real-time collaboration, two control tablets may be used, and data is shared instantly and immediate feedback is provided as needed.

According to the company's website, the series includes a variety of models designed for different security uses, such as:

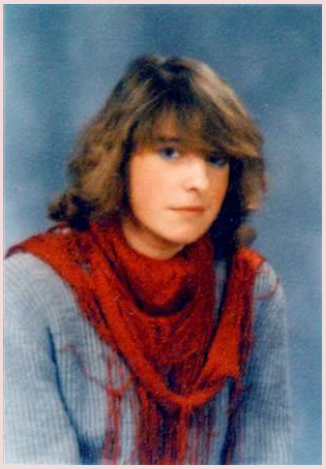
- operations done from a vehicle or on the go. The systems are compatible with an external power supply option for an unlimited operation period.
- operators who need to carry a complete system on the back.
- parachuting, hostile environments or any other direct action (DA) necessities.
- covert work in urban scenarios. This extremely lightweight, compact system allows for a discreet approach to crowded areas, while providing easy deployment and immediate outstanding images.

The company, that sees itself as a quality technology leader, sells its products to police and military sappers all over the world.

Raised as Catholic in Belgium, She Died as a Muslim Bomber

By Craig S. Smith

Source: http://www.nytimes.com/2005/12/06/world/europe/raised-as-catholic-in-belgium-she-died-as-a-muslim-bomber.html?_r=0



December 2005 – Muriel Degauque, believed to be the first European Muslim woman to stage a suicide attack, started out life as a good Roman Catholic girl in this coal mining corner of Belgium known as the Black Country. She ended it in a grisly blast deep inside Iraq last month.

Ms. Degauque, 38, detonated her explosive vest amid an American military patrol in the town of Baquba on Nov. 9, wounding one American soldier, according to an account received from the State Department and given to the Federal Police in Belgium.

Her unlikely journey into militant Islam stunned Europe and for many people was an incomprehensible aberration, a lost soul led astray. But her story supports fears among many law enforcement officials and academics that converts to Europe's

fastest-growing religion could bring with them a disturbing new aspect in the war on terror: Caucasian women committed to one of the world's deadliest causes.

European women who marry Muslim men are now the largest source of religious conversions in Europe, the experts say. While a vast majority of those conversions are pro forma gestures for moderately religious in-laws, a small but growing number are women who willingly adopt the conservative comportment of their fundamentalist husbands.

Most of those in the conservative ranks are motivated by spiritual quests or are attracted to what they regard as an exotic culture.

But for some, conversion is a political act, not unlike the women who joined the ranks of South American Marxist rebels in the 1960's and 1970's.

"They are people rebelling against a society in which they feel they don't belong," said Alain Grignard, a senior official in the antiterrorism division of the Belgian Police. "They are people searching through a religion like Islam for a sense of solidarity."

He said there were many such women married to the first wave of Europe's militant Islamists a decade ago, and some of them followed their husbands to Taliban-ruled Afghanistan. But while they supported their husbands' militancy, he said, they never acted themselves. "This was the first," said Mr. Grignard, "and it's clear there could be others."

French antiterrorism officials have been warning for several years that female converts represent a small but increasingly important part of the terrorist threat in Europe.

As early as May 2003, France's famed antiterrorist investigating judge, Jean-Louis Bruguière, warned that European terrorist networks were trying to recruit Caucasian women to handle terrorist logistics because they would be less likely to raise suspicion.

He said then that it was only a matter of time before the women moved on to more violent acts.

Ms. Degauque was born in the small suburb of Charleroi, a gritty coal and steel town where her father operated a crane at the sprawling smelter, according to neighbors and friends.

She grew up doted on by her mother, Liliane, who worked as a cleaner and monitor at the local elementary school.

"Her mother spoiled her," said Jeannine Beghin, who has known Ms. Degauque's mother since childhood. Ms. Beghin recalled that Ms. Degauque's mother rented out a hall and gave a catered party with music and dancing to celebrate the daughter's first communion.

"Muriel had the prettiest dress of all the girls," Ms. Beghin said.

Her teachers remember her as a well-dressed, well-behaved young woman, even if she was a middling student. "Muriel was more literary than scientific," said Rita Detraux, a retired high school teacher. Still, Ms. Degauque seemed adrift by the time she took an apprenticeship as a sales clerk at a bakery in Charleroi after her third year of high school. The local press has quoted her former boss as saying that Ms. Degauque would disappear at lunchtime, and that he soon learned she was using drugs.

Talk that Ms. Degauque had fallen into the wrong crowd soon circulated in the neighborhood. The Belgian Police say she became known as a drug user, though she was never arrested. In her late teens, she followed her older brother in joining a local motorcycle club, the Apaches, and neighbors saw her come and go in a black leather jacket on the back of a boyfriend's motorcycle.

By most accounts, Ms. Degauque's wayward streak took a decisive turn when her brother was killed in a motorcycle accident

when she was 20. He had always been the more popular of the two, people who know the family say. One neighbor, Andrea Dorange, has told local newspapers that Ms. Degauque said she should have died instead of her brother.

Ms. Degauque soon moved out of the house and began a troubled life in Charleroi. She married a much older Turkish man in what neighbors presumed was an arrangement to help him legalize his status in Belgium. They divorced about two years later.

Ms. Degauque had several boyfriends after that and worked at the restaurant of one for a while. She eventually met an Algerian man who introduced her to Islam. She began appearing at her parents' home wearing a head scarf.

Her mother told neighbors that she was pleased because Islam had helped her daughter stop drinking and doing drugs. But her devotion became disturbing several years later after she met and married Issam Goris, the son of a Belgian man and Moroccan woman. Mr. Goris with his long beard was already known to Belgian Police as a radical Islamist. Ms. Degauque moved with him to Brussels and then to Morocco, where she learned Arabic and studied the Koran.

When she returned, she wore not only a head scarf but the full length robe worn by Muslim women of North Africa. She and Mr. Goris moved to a one-bedroom apartment a few blocks from his mother in the largely immigrant neighborhood near Brussels' Midi train station. The building's owner, who gave his name only as Mahmed, said she collected unemployment checks. It is not clear what her husband did.

As Ms. Degauque became increasingly rigid, she demanded that her parents follow Islamic customs when she and her husband visited, forbidding her father to drink alcohol or the men and women to eat together. Ms. Beghin was at the home when the couple arrived for their last visit about six months ago.

"Muriel came in with nothing but her eyes showing, even wearing gloves," Ms. Beghin said. "When her husband saw me he went immediately through the house and into the backyard." She said Ms. Degauque's mother later explained that he could not bear to be in the presence of a strange non-Muslim woman.

Ms. Degauque's parents did not know that she had left the country until she called them from Syria in August, according to Ms. Beghin. Ms. Degauque told her mother that she would be gone more than a year but the line went dead before her parents could learn more. The Degauques tried repeatedly to reach their daughter on her mobile phone but got only her voice mail.

The Belgian Police now say that Mr. Goris had fallen in with a group of Islamists focused on recruiting European Muslims to fight with Abu Musab al-Zarqawi's terrorist network in Iraq. The police had been monitoring the group for months when they intercepted phone calls from Mr. Goris in Iraq indicating that he and his wife were already there. The Belgians didn't yet know Mr. Goris and Ms. Degauque's identities, but they notified the United States and the Iraqi government that a Belgian couple was in the country intent on carrying out attacks. They turned over information on the telephone calls that would allow the Americans to find Mr. Goris, but Ms. Degauque struck before they did.

Little of Ms. Degauque remained after the explosion in which she died, according to the Belgian Police, though the American soldiersrecovered her passport and other papers. That same day, the Americans found Mr. Goris, who was also wrapped in explosives, apparently about to carry out an attack. They shot him before he could detonate his charges.

The police continued to monitor the Belgian recruiting network after the deaths, hoping to gather enough information to make conclusive arrests. Those plans were interrupted last week when French radio reported Ms. Degauque's death. Belgium quickly arrested 14 people, fearing the report would send them into hiding. The Belgian authorities have released all but five of them, including the 18-year-old girlfriend of a suspect who was also being pressured to leave for Iraq. The Belgian government has asked the United States to send DNA traces that will allow it to confirm that Ms. Degauque is dead, but the Belgian Police say that neither Ms. Degauque's remains nor Mr. Goris's body will be returned.

Craig S. Smith *is a writer at large for The New York Times. He was previously the Times' Managing Director for China where he built and operated the company's first foreign language platforms. Mr. Smith holds a Bachelors degree and Masters degree from Columbia University.*

Children strapped with explosives kill nine in north Cameroon

Source: https://mercury.postlight.com/amp?url=http://news.trust.org/item/20170602103920-f81g9

June 03 – **Two children carrying explosives blew themselves up on Friday near a camp in northern Cameroon housing civilians displaced by Nigeria's Boko Haram militants, killing nine people and wounding 30,** officials said.

They entered the town of **Kolofata**, around 10 km (6 miles) from the border with Nigeria, before dawn, posing as refugees looking for food before the start of the daytime fast for Ramadan.

"Two suicide bomber adolescents **aged between 10 and 15 years** infiltrated the town of Kolofata," Communications Minister Issa Tchiroma Bakary told state radio, adding that both had detonated their explosives.

"The death toll is 1l, including the two suicide bombers, and 30 wounded, of which 10 are seriously wounded," he added.

A local government official said the 10 gravely wounded had been transported to a hospital in a nearby town.

"It was unbearable. People were screaming. Others were moaning. It was total horror," said a policeman present at the scene of the bombing.

Northern Cameroon has in recent years suffered from the overflow of violence linked to Nigeria's Boko Haram Islamist insurgents. Nigerian refugees have flooded across the border and local residents have been forced to flee their homes.

Boko Haram launches frequent cross-border raids in its bid to carve out an Islamic caliphate. Its eight-year insurgency has killed more than 20,000 people in the Lake Chad region and, according to the latest U.N. refugee agency figures, displaced 2.7 million.

The agency said on Friday it was "stepping up its response as large numbers of refugees return from Cameroon to north-eastern Nigeria," including some 12,000 in May, often returning home to very harsh, unsanitary conditions.

Villages and towns in the area have regularly been targeted by bombers. The officials said that Friday's bombing came a day after two young girls detonated their explosives in the nearby village of Djakana, killing themselves and lightly injuring two members of a local civilian self-defence force.

Kolofata has repeatedly been struck in the past, including one attack that killed nine people in September 2015. Nigeria's army has retaken much of the territory once occupied by Boko Haram, and a military coalition of regional neighbours has helped fight the Islamist insurgents across the borders in Niger, Chad and Cameroon.

The Cameroonian government has deployed thousands of soldiers, including elite units, to the Far North region.

U.S. Department of Homeland Security Office for Bombing Prevention-Counter IED Resources Guide

Source: https://tripwire.dhs.gov/IED/resources/docs/OBP_Counter-IED_Resources_Guide.pdf

June 05 – The U.S. Department of Homeland Security's Office for Bombing Prevention (OBP) recently published its newest Counter Improvised Explosive Device (Counter-IED) Resources Guide. The mission of the OBP is to protect life and critical infrastructure by building capabilities within the public population and across the public and private sectors to prevent, protect against, respond to, and mitigate bombing incidents.

Helping explosive detection canine teams across the U.S.

Source: http://www.homelandsecuritynewswire.com/dr20170608-helping-explosive-detection-canine-teams-across-the-u-s

June 08 – Dogs are uniquely suited to sniffing out explosives – their sense of smell is more than a million times stronger than a human's. Harnessing this natural ability to help law enforcement identify explosives requires specialized training and testing. Many detection canine teams, however, have limited access to critical training materials and limited time to establish rigorous training scenarios. S&T says that the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Detection Canine Program has developed an initiative to support these needs for the nation's more than 4,000 explosives detection canine teams.

The DHS S&T Detection Canine Program, part of S&T's Homeland Security Advanced Research Projects Agency's Explosives Division, has created the **Regional Explosives Detection Dog Initiative (REDDI),** a series of events aimed at advancing the knowledge and capabilities of the nation's detection canine teams.

"We are setting up real-world problems," said Don Roberts, DHS S&T Detection Canine Program Manager. "REDDI seeks to improve the operational effectiveness of the law enforcement explosive detection canine teams while informing S&T on where our research investment needs to be focused going forward."

In March 2017, the Detection Canine Program kicked off REDDI to share knowledge and provide exercises in basic odor recognition and realistic operational search scenarios. REDDI began with the first event in Fort Myers, Florida, and moved to Westport, Connecticut, in April. Miami, Florida, is scheduled to host REDDI in late May, and plans are underway to

continue REDDI through 2018. Up to twenty explosives detection canine teams participate in each two-day program, which includes classroom presentations on current explosive threats and the chemistry of explosives, as well as odor recognition trials and operational searches. The goal is to improve explosive detection canine team training effectiveness and efficiency in order to improve overall operational proficiency.

REDDI provides a realistic setting where law enforcement teams from several jurisdictions can evaluate their detection capabilities, understand their strengths, and identify additional training needs. The DHS detection canine research program benefits from REDDI in that it validates current investments and informs the direction of future research. Participation in a REDDI event is often the first opportunity a local law enforcement explosive detection canine team has to assess their capabilities in authentic, real world scenarios, with scientifically rigorous oversight by DHS S&T.

S&T has funded two tools to strengthen the impact of REDDI – non-hazardous peroxide training aids and a custom-developed data collection tool. S&T partnered with the Johns Hopkins University Applied Physics Laboratory to develop non-hazardous, non-detonable canine training aids made with actual peroxide-based explosives through a patented process. These training aids can be used anywhere, require no special handling or storage requirements, and provide explosives detection canine teams more opportunities to train with the peroxides in operational settings.

"The problem is that these are sensitive explosives," said Roberts. "They are difficult to train with, and the teams aren't getting the frequency of training we feel might be necessary to stay proficient. Having non-hazardous training aids allows the teams to train with the peroxide material in the operational environment, like airports, stadiums or in mass transit."

S&T notes that it is also using the Mobile Application for Canine Evaluation, or MACE, a tablet-based data collection tool developed by S&T partner Battelle Memorial Institute, to provide immediate feedback at REDDI events to canine teams and their trainers. MACE compiles performance data in real time, which makes it possible for S&T to efficiently and effectively conduct REDDI as a two-day event.

"The explosives detection canine is the best, most versatile mobile explosive detection tool at our disposal for protecting the Homeland from the explosive threat," said Roberts, "and DHS S&T's mission is to provide tools, techniques and knowledge to better understand, train and utilize explosive detection canine teams in the operational environment."

▶▶ **To learn more about REDDI, read** the program factsheet.

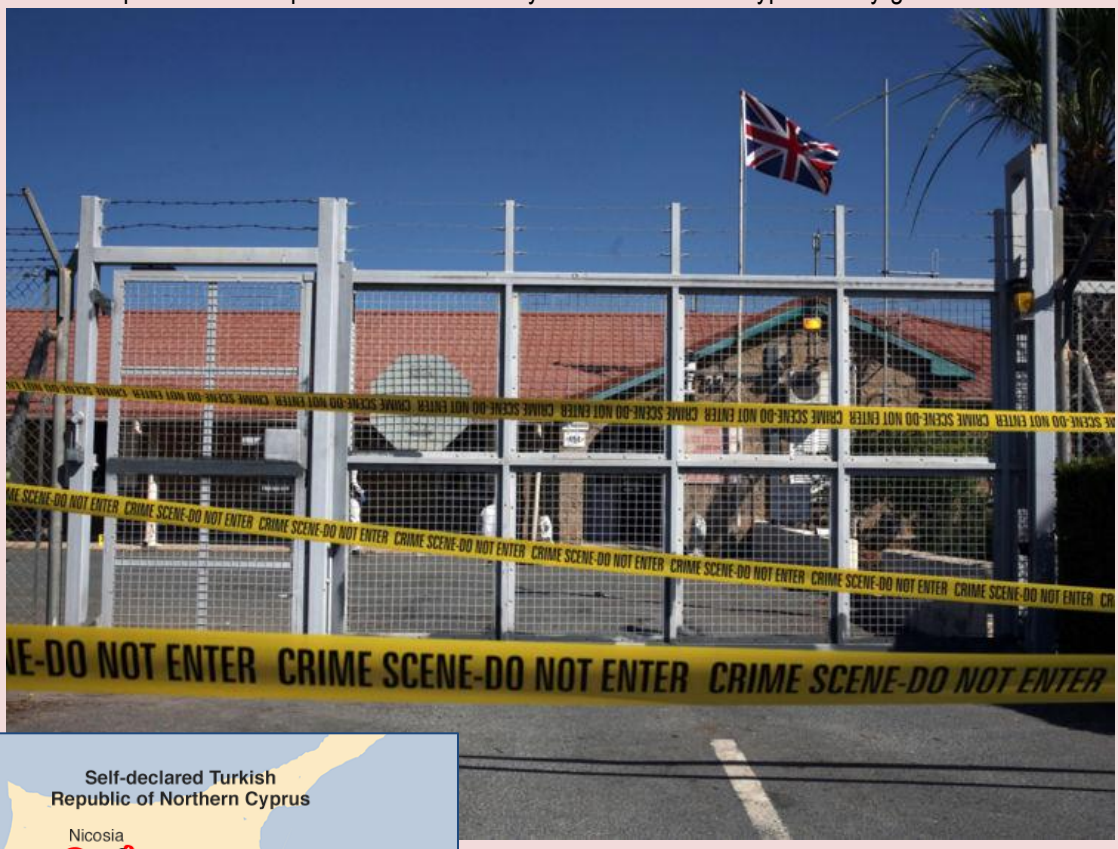
Mass Casualty Explosives Attacks in Iraq and Afghanistan

Source:https://www.start.umd.edu/pubs/START_MassCasualtyExplosivesAttacksIraqAfghanistan_BackgroundReport_June2017.pdf

In the aftermath of a series of deadly terrorist attacks in Baghdad and Kabul involving vehicle bombs, START has compiled information from the Global Terrorism Database (GTD) on terrorism in Iraq and Afghanistan and the use of explosives—particularly vehicle-borne explosives and suicide tactics—in terrorist attacks.

British military's Dhekelia base in Cyprus hit by 'grenade' blast

Source: http://counteriedreport.com/british-militarys-dhekelia-base-in-cyprus-hit-by-grenade-blast



June 13 – **A blast at a British base on the southeast coast of Cyprus has injured a police officer. The explosion struck the Dhekelia garrison before dawn on Tuesday. The Cyprus Mail reported a grenade had been thrown by a man on a motorbike.**

Police spokesperson Kristian Gray said investigations were ongoing and authorities are viewing the explosion as a criminal case.

"The building suffered no structural damage, just a broken window," he added.

A source told the AFP news agency that the attack could be related to the involvement of the base's police in a crackdown on illegal bird trapping.

It reported it came after bird trappers had been handed a "heavy fine" by a court.

More than two million migratory birds are slaughtered each year on the island.

A spokesperson from the Ministry of Defence told Sky News that Sovereign Base Areas Police were investigating an explosive incident which took place in the early hours of the morning at the Dhekelia base.

"At this stage the Police are treating this as a criminal investigation. Until the initial investigation has concluded we will not be in a position to make any further comment," they said.

Cyprus became an independent republic, free from British colonial rule, in 1960, but the UK retains two bases which remain British sovereign territory and house military headquarters.

The sites, at Dhekelia and Akrotiri, cover some 98 square miles of territory and allow the UK to conduct military and humanitarian missions from the eastern Mediterranean.

Israeli intelligence discovered IS plans for laptop bomb

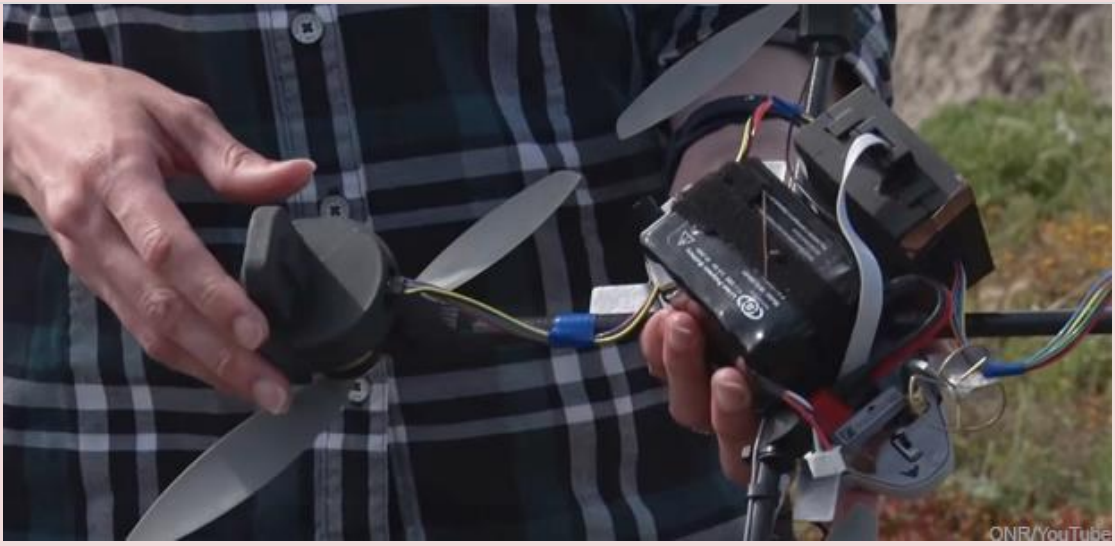
Source: http://www.dailymail.co.uk/wires/afp/article-4597118/Israeli-intelligence-discovered-IS-plans-laptop-ban-report.html

June 12 – Israeli government spies hacked into the operations of Islamic State bombmakers to discover they were developing a laptop computer bomb to blow up a commercial aircraft, The New York Times reported Monday.
The Times said the work by Israeli cyber operators was a rare success of Western intelligence against the constantly evolving, encryption-protected and social media-driven cyber operations of the extremist group.
It said the Israeli hackers penetrated the small Syria-based cell of bombmakers months ago, an effort that led to the March 21 ban on carry-on laptops and other electronics larger than cellphones on direct flights to the United States from 10 airports in Turkey, the Middle East and North Africa.
The Israeli cyber penetration was the source of US information about how the group was developing explosives that couldn't be detected by standard screening because they looked identical to laptop batteries, according to the Times.
The intelligence was so good that it also included the detonation method for the bombs, the Times said, citing two US officials familiar with the operation.
Following the US laptop ban, Britain announced a similar prohibition for flights originating from six countries.
Israel's contribution to the intelligence on the laptop bombs became public after President Donald Trump revealed details of the plot to Russian Foreign Minister Sergei Lavrov in a May 10 White House meeting.
Trump's disclosure "infuriated" Israeli officials, according to the Times.

Flying metal detectors? Navy tests new unmanned mine-detection system

Source: http://counteriedreport.com/flying-metal-detectors-navy-tests-new-unmanned-mine-detection-system

June 01 – During a recent technology demonstration at Marine Corps Base Camp Pendleton, Dr. Rosemarie Oelrich and Dr. Cory Stephanson unveiled a new way to detect buried and submerged mines.
Oelrich, a scientist at Naval Surface Warfare Center (NSWC) Carderock's Combatant Craft Division, and Stephanson, president and chief executive officer of Broadband Discovery Systems (BDS), stared at an Android tablet showing search data from an unmanned aerial drone they had just flown. The device's screen glowed as a green fluorescent map appeared, splashed with red clusters of varying sizes and shapes.
"See that large cluster?" asked Stephanson. "That's the dummy mine we buried. The smaller blotches near it are construction rebar we found nearby. The drone detected and localized these items quickly and accurately, which would be extremely valuable in a real combat scenario."
Oelrich and Stephanson were testing the new Mine Warfare Rapid Assessment Capability (MIW RAC) system. Sponsored by the Office of Naval Research's (ONR) TechSolutions program, **MIW RAC** consists of a one-pound quadcopter outfitted with an ultra-sensitive magnetometer sensor system to detect mines and provide real-time search data to a handheld Android device.
"This technology will help Sailors and Marines who are approaching a beachfront to rapidly clear, or at least determine the location of, mines or other hazards that are in their way," said ONR Command Master Chief Matt Matteson. "It could potentially save a lot of lives."
MIW RAC is a portable, remote-controlled system that can detect buried or underwater mines during amphibious beach landings. It's designed to help explosive ordnance disposal



teams quickly find mines and dangerous metal obstacles within coastal surf zones and very-shallow-water zones. MIW RAC would provide a new, real-time aerial complement to existing underwater mine-detection capabilities.

"Everyone wants to know where they are going and what they are about to get into," said Oelrich, who is overseeing the development of MIW RAC. "It helps to have a rapid capability to just fly something in the air and survey an area before you put troops on the ground or bring a vessel ashore."

While the quadcopter and tablet device are available commercially, the heart of MIW RAC is its proprietary magnetometer sensor suite—which has an extensive detection range and uses complex algorithms to differentiate between various types of objects.

MIW RAC originated in 2015, when the Navy Expeditionary Combat Command (NECC) sent a request to ONR's TechSolutions program for a portable system that could detect potential hazards in surf zones, be easy for warfighters to use and fit diverse platforms. TechSolutions is ONR's rapid-response science and technology program that develops prototype technologies to address problems voiced by Sailors and Marines, usually within 12-18 months.

With TechSolutions guidance, NECC partnered with NSWC Carderock, Combat Direction Systems Activity Dam Neck and two commercial companies—BDS and Physical Sciences, Inc.—to develop the components of MIW RAC.

"We took our inspiration from a stationary scanning system developed by BDS," said Oelrich. "It was sensitive enough to not only detect weapons, but identify the hidden location of the object on a person and the angle in which it was oriented—a knife in a front pocket or gun turned sideways, for example.

"We flipped that concept on its head," she continued. "Instead of a stationary system detecting moving objects, we have a moving system detecting relatively stationary objects."

Later this year, TechSolutions will deliver prototype MIW RACs to NECC's Explosive Ordnance Disposal Group for further testing and evaluation. Oelrich and her team hope to see the system issued throughout the fleet next year.

'Cowardly terrorist attack': 3 women killed in shopping mall blast in Bogota, Colombia

Source: https://www.rt.com/news/392807-colombia-bogota-shopping-mall-blast/

June 17 – The powerful explosion that rocked a shopping center in the Colombian capital's tourist district has been called a terrorist attack by Bogota's mayor. **At least three women, including a French volunteer, died in the blast. Several others were seriously injured**.

Bogota Mayor Enrique Peñalosa has tweeted that three women were killed in the *"bomb"* blast, and one more remains in serious condition. Peñalosa has called the explosion a *"cowardly terrorist attack."*

The explosion targeted the Centro Andino Mall in the Zona Rosa neighborhood, which is regarded as one of the most luxurious upper-class and tourist districts in Latin America. The blast occurred in the women's restroom on the mall's second floor.

One of the victims has been identified as a 23-year-old French woman who had spent six months volunteering in Colombia. The woman, who is said to have worked in a poor Colombian neighborhood, was reportedly killed days before her planned return to France.

The other two victims, who have been identified in a hospital statement as a 31-year-old woman and a 27-year-old woman, are believed to be Colombian. The statement said one woman remains in critical condition.

Earlier, extremely graphic images of seriously injured women and a video showing a smoke-filled mall corridor appeared on social media.

RT Spanish earlier cited police as confirming at least 11 injuries were caused by the blast.

Ambulances and fire engines are working at the scene, and the entire mall has reportedly been evacuated.

Colombian President Juan Manuel Santos strongly condemned the attack, announcing that he was returning to the capital to take charge of the situation.

France's ambassador to Colombia, Gautier Mignot, tweeted that he is *"shocked by the death"* of a French woman in the blast and vowed to provide support for the victim's family.

Meanwhile, messages of condolences for the victims and words of support for the Colombian government have started pouring in. The Mexican government said it *"expresses its solidarity with the people and the government of Colombia,"* and *"deplores the loss of human lives."*

Meanwhile, the National Liberation Army (ELN), a guerrilla group engaged in an ongoing armed standoff with government forces, denied responsibility for the attack.

"ELN-Paz repudiates the attack on Centro Comercial Andino against civilians. We share the pain and we sympathize with the victims," the group's negotiators wrote on its official Twitter account.

In February, ELN claimed responsibility for the bomb attack in Bogota, in which a police officer was killed and dozens of people were injured, including civilians.

Brussels Central Station: Soldiers shoot suspected bomber dead after reports of explosion

Source: http://www.abc.net.au/news/2017-06-21/brussels-central-station-evacuated-following-reports-of-blasts/8636984

June 20 – Belgian authorities said they foiled a "terror attack" when **soldiers shot dead a suspect after a small explosion at a busy Brussels train station** that continued a week of attacks in the capitals of Europe.

Federal prosecutor Eric Van der Sypt said soldiers "neutralised" a male suspect at the Central Station immediately after the explosion.

The man lay still for several hours while a bomb squad checked whether he was armed with more explosives.

The prosecutor's spokeswoman Ine Van Wymersch confirmed his death and said no other explosives were found on his body.

A public prosecutor, quoted by local media, said the man was wearing an explosive belt.

"An individual carrying a rucksack and an explosive belt in Central Station has been shot dead," the prosecutor said.

Belgian federal prosecutors said the incident was being treated as a terrorist attack. The national alert level was maintained at its second-highest level.

A police spokesman said there was an explosion around a person before they were "neutralised by the soldiers that were on the scene".

Mr Van der Sypt said the man appeared to be 30 to 35 years of age but authorities had "no idea of his identity".

Local media reported that a bomb squad had performed a controlled explosion of an explosive belt the suspect had at the Central Station, and was checking to see if there were more hazards.

Station employee Nicolas Van Herrewegen told public broadcaster RTBF that he saw a man shouting in a lower level of the 1930s station, which serves lines running under the city centre.

He then appeared to yell "Allahu Akbar", Arabic for "God is great", and to detonate something on a luggage trolley.

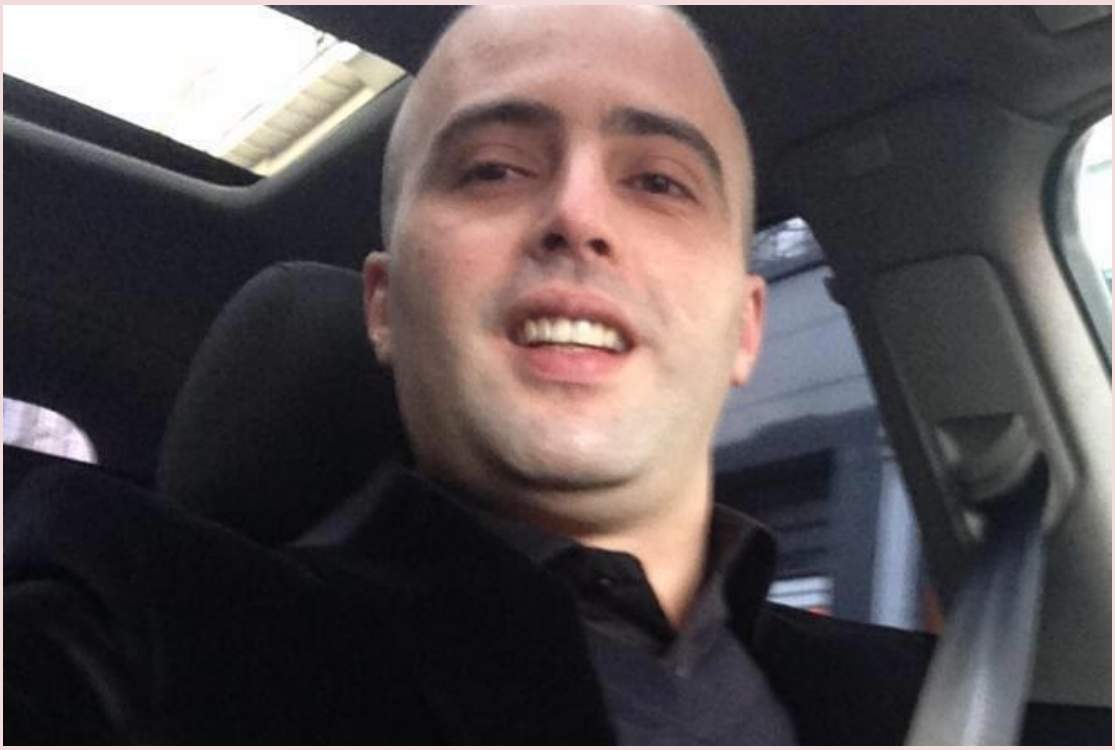
People standing within three metres of the trolley were unhurt, Mr Herrewegen said.

Reporters at the scene a little over an hour after the incident said the area was quiet, with police manning a cordon and a few bystanders calmly watching security forces at work.

Rail company spokeswoman Elisa Roux said that trains were being diverted from the station and replacement buses sent out to take passengers to the area.

.The station and the adjacent historic downtown area Grand Place square, packed with tourists and locals on a hot summer evening, were evacuated as police set up a security cordon, witnesses told Belgian media.

The city has been on high alert for more than 18 months since Brussels-based Islamic State militants carried out attacks in Belgium and France.



Moroccan Oussama Zariouh, 36, screamed "Allahu akbar" at soldiers and charged at them before being killed in a hail of gunfire

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

Creating high-speed internet lane for emergency situations

Source: http://www.homelandsecuritynewswire.com/dr20170525-creating-highspeed-internet-lane-for-emergency-situations

May 25 – **In a disaster, a delay can mean the difference between life and death. Emergency responders don't have time to wait in traffic — even on the congested information superhighway.**

This is why researchers at Rochester Institute of Technology are developing a faster and more reliable way to send and receive large amounts of data through the internet. By a creating a new network protocol, called **Multi Node Label Routing protocol**, researchers are essentially developing a new high-speed lane of online traffic, specifically for emergency information.

RIT says that the project, funded by a grant from the National Science Foundation and U.S. Ignite, aims to improve the information flow between emergency responders at the scene of an incident and decision-makers at the office of emergency management.

"Sharing data on the internet during an emergency is like trying to drive a jet down the street at rush hour," said Jennifer Schneider, the Eugene H. Fram Chair in Applied Critical Thinking at RIT and co-principal investigator on the project. "A lot of the critical information is too big and data heavy for the existing internet pipeline."

Schnieder said data-dense information sharing was a major issue during recent disasters, including Hurricane Irene and Hurricane Sandy. Emergency responders were not able to quickly share critical information. That's why RIT students studying environmental health and safety — several of whom are actual responders themselves — worked with emergency professionals to gather data and create scenarios that support research into this real-world problem.

For example, in a flood event, emergency responders may need to share LIDAR mapping images, 911 requests and deployments, cell phone location data, video chats, voice recordings and social media communications. When that information has to compete with civilians tweeting about the disaster and messaging loved ones, the network is taking on more than it can handle.

"It is normal to have links and routers fail, and as the network topography changes, packets can be delayed, rerouted or lost," said Nirmala Shenoy, a professor in RIT's Information Sciences and Technologies Department and principal investigator of the project. "This unreliability and delayed information can render loss of important data in the LIDAR images and other information."

To solve this problem, Shenoy, along with co-principal investigator Erik Golen, a visiting assistant professor in RIT's Information Sciences and Technologies Department, and a team of five graduate students created the Multi Node Label Routing (MNLR) protocol. It is designed with an immediate failover mechanism—meaning that if a link or node fails, it uses an alternate path right away, as soon as the failure is detected. The new protocol runs below the existing internet protocols, allowing normal internet traffic to run without disruption.

The new protocol does not depend on routes discovered by either Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF). It discovers routes based on the labels assigned to the routers. The labels in turn carry the structural and relational connectivity information among routers.

"The new protocol is actually of very low complexity compared to the current routing protocols, including BGP and OSPF," Shenoy said. "This is because the labels and protocols leverage the connectivity relationship that exists among routers, which are already sitting on a nice structure."

In a demo this May, the team put the protocol to the test over the U.S. GENI (Global Environment for Network Innovation). The group transferred data using BGP and the new MNLR protocol. They ran the data between 27 nodes representing the network of the incident control center, the 911 call center and the office of emergency management.

While BGP took about 150 seconds to recover from a link failure, MNLR recovered in less than 30 seconds. The recovery metrics showed that the new MNLR protocol transferred information faster and more reliably than existing protocols in the event of network failures and topology changes.

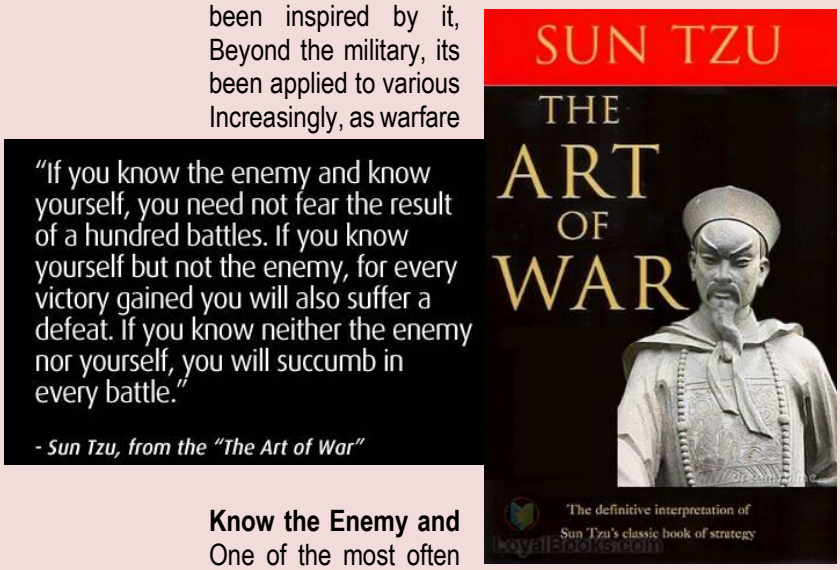
"While BGP has a recommended default keep alive message interval of 60 seconds, MNLR is

not so constrained," said Shenoy. "In fact, MNLR can detect failure with one missing keep alive message as the failure or topology change information will be flooded internet wide, which can be expected in certain cases with BGP."
Shenoy said that the main issue with current protocols stems from the fact that they were invented several decades ago and not for the type of network scenarios experienced in current internet. Thus, BGP and OSPF are unreliable and that manifests when a link fails, she said.
"If you receive an email five minutes late, that is still acceptable," Shenoy said. "But in an emergency situation, the implicit impact of these serious network problems truly come to light."
In an emergency situation, information becomes too old after about eight minutes, adds Schneider, who leads RIT's Collaboratory for Resiliency and Recovery. "We are on the cusp of generating and collecting all this great technical information, but we need to be able to share it and create the situational awareness decision-makers need."
RIT notes that the team is continuing to develop and enhance the MNLR protocol. In the future, the team plans to test and implement the protocol in emergency situations.

Sun Tzu's 'The Art of War' for Cybersecurity

By Tom Madsen (Security Advisor, Fort Consult)
Source: https://www.infosecurity-magazine.com/opinions/sun-tzus-art-of-war-cybersecurity/

May 29 – An ancient Chinese military treatise from the 5th century BC, The Art of War by Sun Tzu, is considered a definitive work on military strategy and tactics. Through the ages, military leaders have been inspired by it, even to this day.
Beyond the military, its advice on how to outsmart opponents has been applied to various competitive fields from business to sports.
Increasingly, as warfare moves from the battlefield to the realm of cyber-space, its principles are being seen as especially applicable to cybersecurity.



Despite being written thousands of years ago, these classic defense strategies are undoubtedly still relevant for the modern defender of IT infrastructure. The principles of Sun Tzu are not only relevant to defense, but also for understanding the approach of attackers.

Know the Enemy and Know Yourself

One of the most often quoted Sun Tzu quotes has enduring resonance for many situations in life, including cybersecurity. To understand how a hacker is likely to operate, we must first understand their motivations and what they are trying to achieve. When we know what assets they are likely to target, we can better focus on effectively protecting them.
To be properly prepared for cyber-incidents, we must also have a clear understanding of our own business and infrastructure – where is our data held? What software are we running? Is everything patched and maintained? What's more, is the proper training in place for staff? Attackers will always 'strike at what is weak,' and employees are often the weakest link in the security chain.

All Warfare is Based On Deception

Many of the methods used by attackers are based on deception – whether that's phishing, spear phishing, whaling or social engineering. Often used to trick unsuspecting employees into engaging with malicious attachments or links, phishing attacks are becoming increasingly sophisticated – with hackers now tricking employees by posing as more senior members of staff and even CEOs, requesting funds to be transferred.
Recent ISACA research has found that 1 in 5 UK office workers have fallen prey to phishing scams, while over half said their employer has not provided any cybersecurity awareness

training. Employee training and awareness is key to limiting the risk of deception by malicious attackers – and as the above example demonstrates, this training needs to be rolled out to the most senior staff, too.

Attack him Where he is Unprepared, Appear Where you are Unexpected

While employees can be a weak link in the chain, they are not the only route inside an organization. It's important to remember that attackers will also have been trained to know their enemy and, in preparation for an attack, will have done their homework on all possible routes and weaknesses. Organizations should therefore consider all avenues of access and what vulnerabilities they might have.

Fortunately with exercises such as penetration testing, organizations are now able to assess their own security before a hacker does. Through this exercise, organizations can not only scan their systems for vulnerabilities, they can also test employee knowledge and awareness by simulating a real-world attack scenario.

Just As Water Retains No Constant Shape, In Warfare There Are No Constant Conditions

Attackers are agile, so organizations need to be as well. As organizations become wise to traditional attack methods, hackers will only develop new ones in a constant arms race for supremacy.

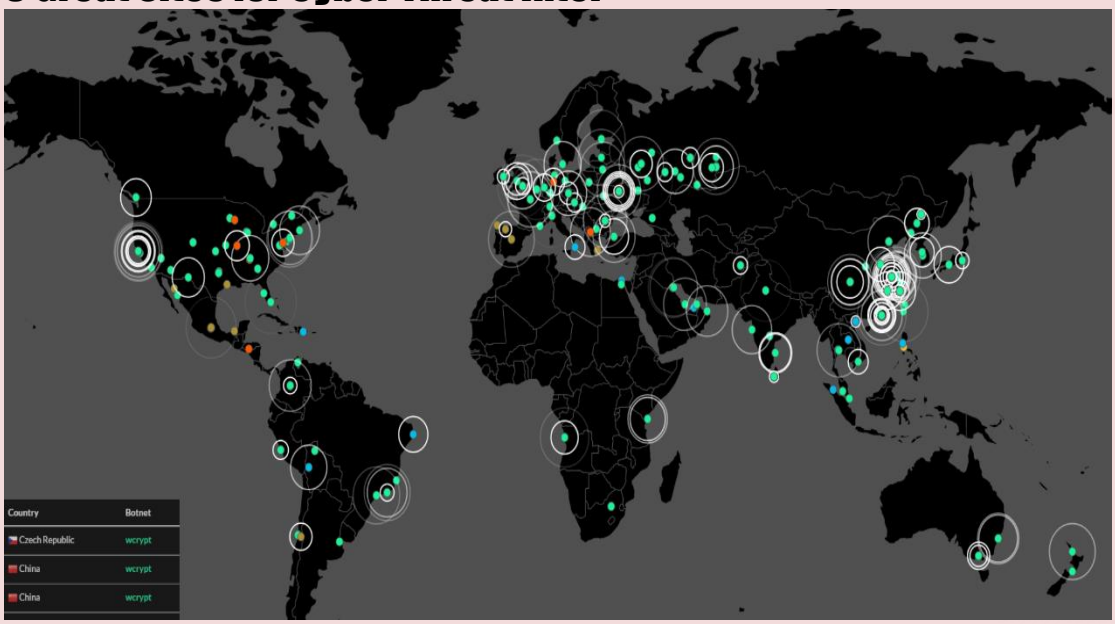
At the same time, businesses are continually evolving and adapting – whether that's upgrading systems, introducing new technologies or changing business models. Businesses should be mindful that all of this change can introduce new cyber security risks, or remove old ones. One of the best ways to be prepared is to keep up to date with the latest best practice frameworks for enterprise IT, such as COBIT 5.

In the Midst of Chaos There Is Also Opportunity

When it comes to cybersecurity breaches, the rule is always 'when,' not 'if.' When breaches occur, organizations should focus on the lessons they can learn and improvements they can make as a result. The root cause should be identified and changes should be swiftly implemented to address this, with the lessons learned shared with all relevant staff.

Suffering a breach can provide the opportunity to reflect and revisit the strategies organizations have in place. Why not apply strategies that have been tried and tested over millennia? **As Sun Tzu says, "The opportunity to secure ourselves against defeat lies in our own hands".**

8 Great Sites for Cyber Threat Intel



Source: https://www.linkedin.com/pulse/8-great-sites-cyber-threat-intel-ely-kahn?trk=v-feed&lipi=urn:li:page:d_flagship3_feed;wd0trEkHVmBEZXlQegSdYA%3D%3D

Hackers could take control of missiles on U.K. subs, start a "catastrophic" nuclear war: Report

Source: http://www.homelandsecuritynewswire.com/dr20170602-hackers-could-take-control-of-missiles-on-u-k-subs-start-a-catastrophic-nuclear-war-report

June 02 – **Hackers could take control of nuclear weapons-carrying Vanguard-class submarines and start a "catastrophic" nuclear war, a new report warns.**

Britain's Trident nuclear weapons deterrent program consists of four Vanguard-class submarines, each carrying up to sixteen Trident II D5 ballistic missiles with a nuclear warhead.

A report from the British American Security Information Council (BASIC) has pointed out disturbing security vulnerabilities in the U.K.'s nuclear weapons program. If exploited, these security flaws could lead to devastating loss of life and would render Britain defenseless against attack.

Fox News reports that the 38-page BASIC report warns a security breach could "neutralize operations, lead to loss of life, defeat or perhaps even the catastrophic exchange of nuclear warheads (directly or indirectly)."

The report's authors note that technological advances – advances which capable hackers could exploit – now move forward so rapidly, that even a nuclear weapons-carrying sub equipped with the best security measures available, could now be vulnerable to cyberattack.

The report stress that lone hackers and cyber criminals likely do not have the skills or capabilities to "conduct operations of the required scale and sophistication relevant to penetrating Trident systems."

Such an attack would require the capabilities and sophistication of a nation-state.

"We are not talking about a lone wolf teenager in a basement hacking into the controls of a missile and warhead and starting a nuclear war," the researchers said.

"Rather, we consider the most significant threat by some margin originates from the expanding investments by leading states in their offensive cyber capabilities, alongside their existing intelligence networks."

The subs, which spend more than half the time submerged, are not connected to the internet and are difficult to track down or hack, something the authors acknowledge.

"Submarines on patrol are clearly air-gapped, not being connected to the internet or other networks, except when receiving (very simple) data from outside. As a consequence, it has sometimes been claimed by officials that Trident is safe from hacking."

But this does not mean that the submarines are immune to hacking. To make this claim – as the Ministry of Defense does, "is patently false and complacent," they researchers say.

The submarine do return to port for routine maintenance and refurbishment, and the report's authors say that when in port, the subs could be "injected" with malicious software. This malware may lie dormant, waiting be activated remotely at the time of the hacker's choosing.

"Trident's sensitive cyber systems are not connected to the internet or any other civilian network. Nevertheless, the vessel, missiles, warheads and all the various support systems rely on networked computers, devices and software, and each of these have to be designed and programmed. All of them incorporate unique data and must be regularly upgraded, reconfigured and patched."

Depending on the malware capabilities, it could allow the hackers, presumably working for a nation-state, to disable the launch mechanism of the nuclear arms on board at times of war, the report warned.

"Relying as it does upon numerous computers, complex software and endless lines of code, the Trident system is undeniably vulnerable to cyber interference," the report said.

Des Browne, former U.K. Defense Secretary, told the *Guardian* that the threat of nuclear submarine hacking should be taken seriously.

"The WannaCry worm attack earlier this month affecting 300,000 computers worldwide, including vital NHS services, was just a taste of what is possible when cyber-weapons are stolen," he said.

"To imagine that critical digital systems at the heart of nuclear weapon systems are somehow immune or can be confidently protected by dedicated teams of network managers is to be irresponsibly complacent."

The report was written by Stanislav Abaimov, a researcher in

cybersecurity and electronic engineering at the University of Rome and a graduate of the Moscow State Institute of Electronics and Mathematics, and Paul Ingram, Basic's executive director.

Abaimov told the Guardian: "There are numerous cyber vulnerabilities in the Trident system at each stage of operation, from design to decommissioning. An effective approach to reducing the risk would involve a massive and inevitably expensive operation to strengthen the resilience of subcontractors, maintenance systems, components design and even software updates. If the U.K. is to continue deploying nuclear weapon systems this is an essential and urgent task in the era of cyberwarfare."

— Read more in Stanislav Abaimov and Paul Ingram, Hacking U.K. Trident: A Growing Threat (British American Security Information Council [BASIC]), June 2017).

Cybercrime to cost global business more than $8 trillion in the next five years

Source: http://www.homelandsecuritynewswire.com/dr20170602-cybercrime-to-cost-global-business-more-than-8-trillion-in-the-next-five-years

June 02 – A new report by Juniper Research has found that **criminal data breaches will cost businesses a total of $8 trillion over the next five years,** due to higher levels of internet connectivity and inadequate enterprise wide security.

The new research, The Future of Cybercrime & Security: Enterprise Threats & Mitigation 2017-2022, forecasts that the number of personal data records stolen by cybercriminals will reach 2.8 billion in 2017, almost doubling to five billion in 2020, despite new and innovative cybersecurity solutions emerging. It highlights cybersecurity problems becoming particularly acute when businesses integrate new and old systems without regard to overall network security.

SMEs pose key risk

Juniper found that SMEs (small and medium enterprises) are particularly at risk from cyberattacks, spending less than $4,000 on cybersecurity measures this year. **Only marginal increases in security spend are expected over the next 5 years.** These firms also tend to run older software, which WannaCry and other recent cyberattacks have exploited.

The research highlights a need for companies to put more money into cybersecurity and system upkeep, which should be treated as a vital element of workplace safety.

"The attacks on hospital infrastructure show that inadequate cybersecurity can now cost lives as well as money,"remarked research author James Moar. "Businesses of all sizes need to find the time and budget to upgrade and secure their systems, or lose the ability to perform their jobs safely, or at all."

Ransomware-as-a-Service is here

Juniper's threat analysis shows that ransomware is becoming a far more advanced form of malware, as ransoming stored data and devices becomes easier and more valuable than stealing financial details.

Juniper expects ransomware to rapidly develop into simple-to-use toolkits, the same way banking Trojans developed into 'products' that required little or no programming knowledge to use.

The whitepaper, Cybercrime & the Internet of Threats 2017, is available to download from the Juniper Research website, together with further details of the new research.

Russian government hackers planted false news story which caused Gulf crisis

Source: http://www.homelandsecuritynewswire.com/dr20170607-russian-government-hackers-planted-false-news-story-which-caused-gulf-crisis-u-s-intelligence

June 07 – U.S. intelligence officials say Russian government hackers planted a false news story into the text prepared for release by the official Qatari news agency.

The release of the Russian-manufactured story by the official Qatari news agency prompted Saudi Arabia and several of its regional allies to suspend diplomatic relations with Qatar and impose economic sanctions on it. U.S. officials say the Russian goal appears to be to cause rifts among the U.S. and its allies.

U.S. intelligence officials say Russian government hackers planted a false news story into the text prepared for release by the official Qatari news agency. The release of the Russian-manufactured story by the Qatari official news agency prompted Saudi Arabia and several of its regional allies to suspend diplomatic relations with Qatar and impose economic sanctions on it.

CNN reports that FBI cyber experts visited Qatar in late May to analyze a cyber breach which involved the Russian hackers placing a fake story with Qatar's state news agency.

Saudi Arabia, already irritated with Qatar's policies on several regional issues, then referred to the Russian-manufactured false report as the "last straw," leading it and its Gulf allies to impose a diplomatic and economic blockade of Qatar.

The blockade is much tougher than similar measures Saudi Arabia and its Gulf allies took in 2014.

The Qatari government said that the 23 May false news report quoted the emir of Qatar as making friendly remarks about Iran and Israel. The fake news story also quoted the emir as questioning how long President Donald Trump would last in office.

But the emir never uttered these words. Rather, Russian government hackers managed to insert the false story into the text prepared for release by the official Qatari news agency.

The Qatari foreign minister, Sheikh Mohammed bin Abdulrahman al-Thani, told CNN that the FBI had confirmed the hack and the planting of fake news.

"Whatever has been thrown as an accusation is all based on misinformation and we think that the entire crisis is being based on misinformation," he said. "It was started based on fabricated news, being wedged and being inserted in our national news agency, which was hacked and proved by the FBI."

Sheikh Saif Bin Ahmed Al-Thani, director of the Qatari Government Communications Office, confirmed that Qatar's Ministry of Interior is working with the FBI and the United Kingdom's National Crime Agency on the ongoing hacking investigation of the Qatar News Agency.

"The Ministry of Interior will reveal the findings of the investigation when completed," he told CNN.

Saudi Arabia, Egypt, the United Arab Emirates, and Bahrain announced on Monday they were severing diplomatic relations and closing air, sea, and land links with Qatar.

They accused the small but rich Gulf state of supporting and financing extremist and terrorist groups, and said Qatar was supporting the regional agenda of Iran.

U.S. officials told CNN that the Russian goal appears to be to cause rifts among the U.S. and its allies.

Cybersecurity on the fly

Source: http://www.homelandsecuritynewswire.com/dr20170605-cybersecurity-on-the-fly

June 05 – When we think of cybersecurity, we think of applying protection measures to our desktop computers such as installing antivirus programs and using passcodes and pin numbers. Just like our computers, aircraft systems are vulnerable and are not exempt from a cyber-attack.

Advancements in technologies are growing at an unprecedented speed and the Air Force has been able to become more innovative and agile using those new technologies. Yet at the same time the risks of being exposed to computer bugs or hacking is increasing and adversaries are becoming more inventive and clever in attacking those systems.

"Aircraft are not immune to being hacked and if they are, it can be detrimental," said Dr. Raju Patel, Air Force Life Cycle Management Center's (AFLCMC) technical advisor for embedded computer and software systems and authorizing official for aircraft systems assessing cybersecurity risks for Air Force aircraft.

Patel said most aircraft systems are now controlled by software and over the years there has been a significant increase of how much is controlled by that software. In the 1980s, approximately 25 percent of the

aircraft's capabilities were operated by software. **Presently, 85 percent of aircraft capabilities are now being ran by software.**

WPAFB notes that if hacked, some examples of possible cyber effects on aircraft systems can be anything from breakdowns in communication and navigation systems to the more critical systems such as collision avoidance and life support systems.

When Patel conducts risk assessments on aircraft systems, he assesses by judging the confidentiality, integrity and availability of the system. Patel said that confidentiality assures that the information is not being disclosed to unauthorized personnel. The integrity of the system is ensuring that the material is what was expected and has not been altered, and that availability insures the user timely and reliable access to data and information services.

Patel said the most important action in protecting aircraft systems as well as other computer systems from a cyber-attack is practicing cyber hygiene.

"Cyber hygiene in avionics needs to begin with ensuring the appropriate training is being provided and the training is tailored to that specific job," Patel said. "Operators also need to ensure that routine maintenance is conducted on the systems by running up-to-date antivirus software and to run the antivirus on any software before it is loaded on the aircraft. It is also crucial that operators follow the technical order as most errors occur when procedures are not followed.

Looking ahead, Patel said additional steps are being implemented to protect aircraft avionic systems from cyberattacks.

Patel created a cybersecurity technical working group collaborating with industry to come to agreeable requirements for the systems. One requirement is to ensure that when contractors provide software, they are vigilant of supply chain issues for any re-used, non-developmental or sub-contracted software, that is who or where the software is coming from.

Another action is installing cybersecurity on the front end of developing weapon systems. **The KC-46 is the first aircraft to address cybersecurity measures during initial system design, and throughout the system development, to protect the aircraft from potential cyber-attacks.**

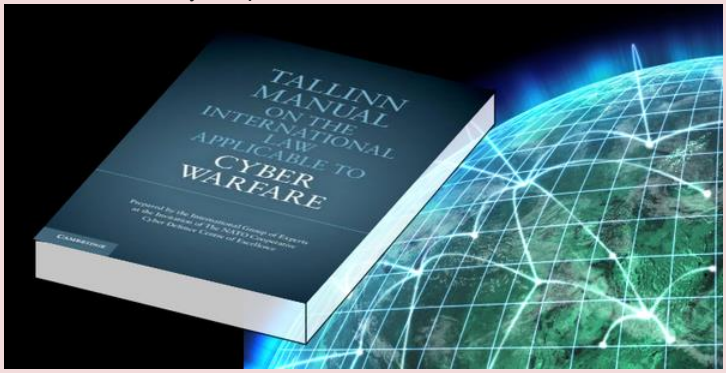
"Adversaries are always looking for ways to hack a system and even if only one small change is made to a system, it can affect the entire weapon system," Patel said.

Patel said that a next generation antivirus program is currently being developed and will have the capabilities to detect and identify malware in real time.

The rulebook for cyberwar

Source: http://technology.iafrica.com/news/1050724.html

June 10 – With ransomware like "WannaCry" sowing chaos worldwide and global powers accusing rivals of using cyberattacks to interfere in domestic politics, the latest edition of the world's only book laying down the law in cyberspace could not be timelier.



The **Tallinn Manual 2.0** is a unique collection of law on cyber-conflict, says Professor Michael Schmitt from the UK's University of Exeter, who led work on the tome. Published by Cambridge University Press and first compiled by a team of 19 experts in 2013, the latest updated edition aims to pin down the rules that governments should follow when doing battle in virtual reality.

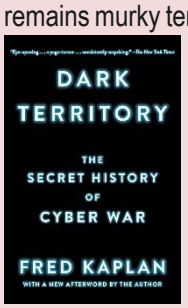
The manual was among the hot topics this week as over 500 IT security experts from across the globe gathered at NATO's Cycon cyber security conference in Tallinn.
Launched in 2009, the annual event is organised by NATO's Cooperative Cyber Defence Centre of Excellence based in the Estonian capital.
In 2007, Estonia was among the first countries to suffer a massive cyber attack, with authorities in Tallinn blaming the Baltic state's Soviet-era master Russia.
"The very next year, in the war between Russia and Georgia, again we saw a lot of cyber activity," said Schmitt, speaking to AFP at Cycon.
Estonia was targeted just three years after it joined NATO and the EU in 2004.
The attack raised a slew serious questions about how to apply and enforce NATO's Article 5 collective defence guarantee in cyberspace, said Schmitt, who also chairs the Stockton Center for the Study of International Law at the United States Naval War College.
He said that NATO allies faced an unprecedented dilemma: did the attack "mean that NATO states had to somehow come to the rescue of Estonia or not?"
Was it "an attack on the civilian population, a violation of international humanitarian law or not? No one had the answers," he added.
"Because of that (attack) the international community started looking at cyber, going: 'Oh my God, I can't answer any question!' That's why this manual was started."

'Digital wild west'
Schmitt says his team's work is intended to tame the "digital wild west" that emerged with the advent of cyberspace.
But the virtually limitless range of possibilities in cyber-conflict raises a long laundry list of legal questions and dilemmas and the Tallinn Manual certainly cannot answer them all.
The legal experts, mostly professors of international law, filled its 642 pages with existing jurisprudence applying to cyberspace from across the globe, and did not shy away from laying out conflicting views on certain issues.
For example: should cyber-espionage be subject to the same laws as conventional spying? Can a state obtain the online IDs and passwords of prisoners of war and use them?
Does a cyberattack trigger a legitimate right to self-defence? Can you retaliate? What kind of status do victims have? What can you do when there is no evidence to prove guilt when attackers can easily cover their tracks?
"This book is intended to be a secondary source of law: it explains the law, but it doesn't create it. States make law," Schmitt told AFP.
"My goal is that this books sits on the desk of every legal advisor for defence and foreign ministers, the intelligence services, so that legal advisors can sit with policy makers and say: in this situation, we can do this, or the law is not clear, you need to make a political decision here.
"But at least the discussion is mature. It's not 'oh my God, what's happening to us?'."

3 Books That Help Make Sense of Cyberwar

Source: https://www.nytimes.com/2017/05/24/books/review/newsbook-cyber-war.html?_r=0

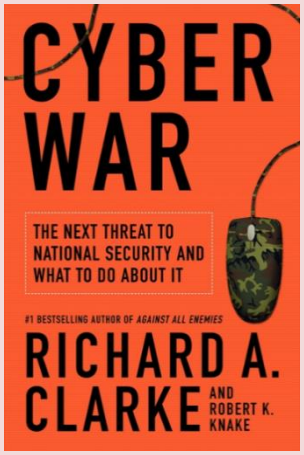
June 10 – The fear of a massive cyber attack became fact on May 12, when over 200,000 computers were hacked in a global blackmail attempt. Hospitals were locked out of medical records; individuals were prompted to pay a ransom in order to access their computers. Yet cyber war and, as such, cyber security, remains murky territory. These books address the cyber threat — and one, published decades ago, shows that the cyber world may have been foreseen in literature.



DARK TERRITORY (2016)
The Secret History of Cyber War By Fred Kaplan
338 pp.

Fred Kaplan draws from conversations with prominent American government leaders, including former directors of the National Security

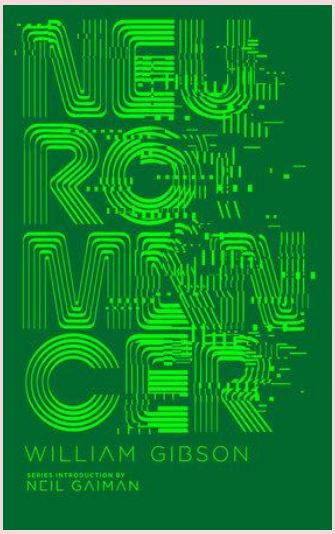
Agency, to deliver a behind-the-scenes look at policy formulation over the last several decades. Kaplan writes: "If America, or U.S. Cyber Command, wanted to wage cyber war, it would do so from inside a glass house." Anything we can do, he argues, adversaries could replicate or learn to do better. (The May 12 cyberattack used technology that originated in the United States.) The book traces the United States' advances in cybersecurity, and Kaplan concludes that though a fair amount of effort is put into developing cyberoffenses, less is focused on protecting the country from potential attacks.



CYBER WAR (2010)
The Next Threat to National Security and What to Do About It
By Richard A. Clarke and Robert K. Knake
290 pp.

Richard A. Clarke, a former counterterrorism adviser to President George W. Bush who criticized the president for ignoring his pre-9/11 warnings about a looming Al Qaeda threat, argues that more resources should be invested into warding off cyberattacks. Though the government has set up protections for intelligence and military information, the private sector remains vulnerable. Clarke and his co-author outline what a cyberattack in the United States might actually look like — trains would be disabled, the financial system and electrical power grids damaged, medical records wiped out. Clarke and Knake lay out a plan they argue will give the United States a fighting chance.

NEUROMANCER (1984)
By William Gibson
304 pp.



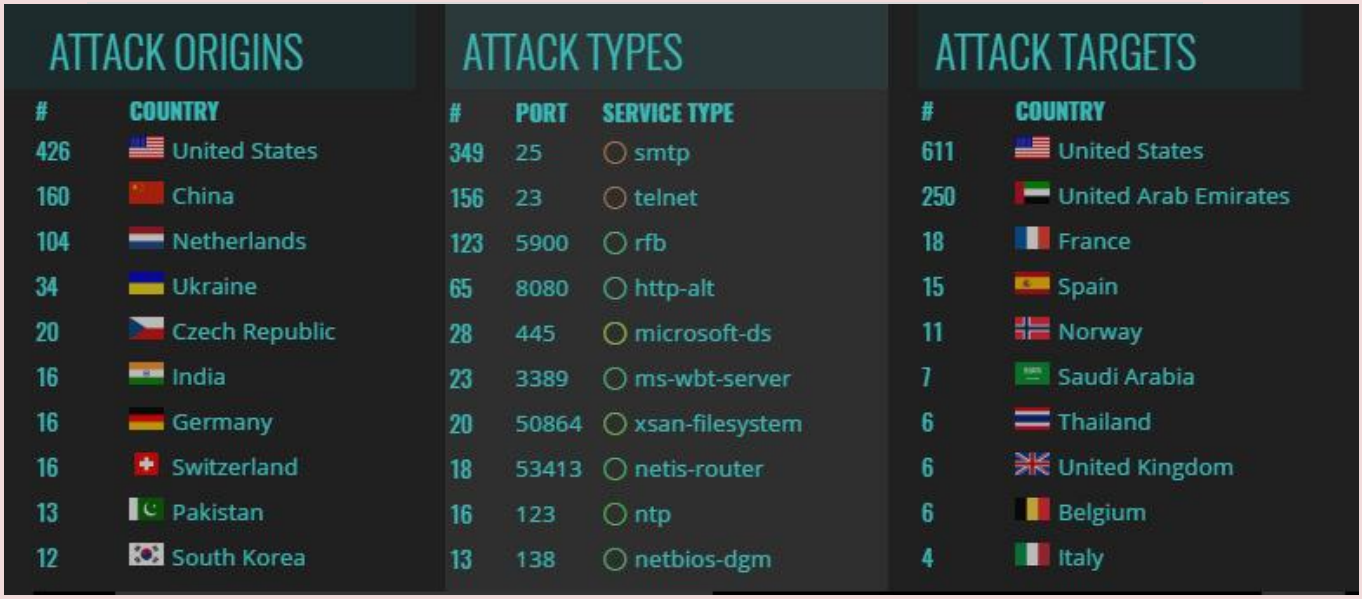
Don't be put off by this book's date of publication; though it appeared before the advent of the World Wide Web, William Gibson's seminal work is eerily prescient. Much of the book takes place in cyberspace, an expression Gibson coined and defined as a "graphic representation of data abstracted from the banks of every computer in the human system." Gibson's protagonist, Case, is a computer hacker who can plug into his machine to intimately experience the electronic transmissions — in other words, enter "the matrix," another term conceived by Gibson. After Case is caught stealing by his former employers, they damage his central nervous system, cutting off his access to cyberspace. When he is offered help repairing his nervous system in exchange for his hacking services in a nefarious mission, Case jumps at the chance. And so begins the novel's swift unfolding. The canonical book explores the implications of increasingly powerful artificial intelligence.

Watch Cyberwar in Real-Time on This Live Map

Source: http://www.visualcapitalist.com/watch-cyberwar-live-map/

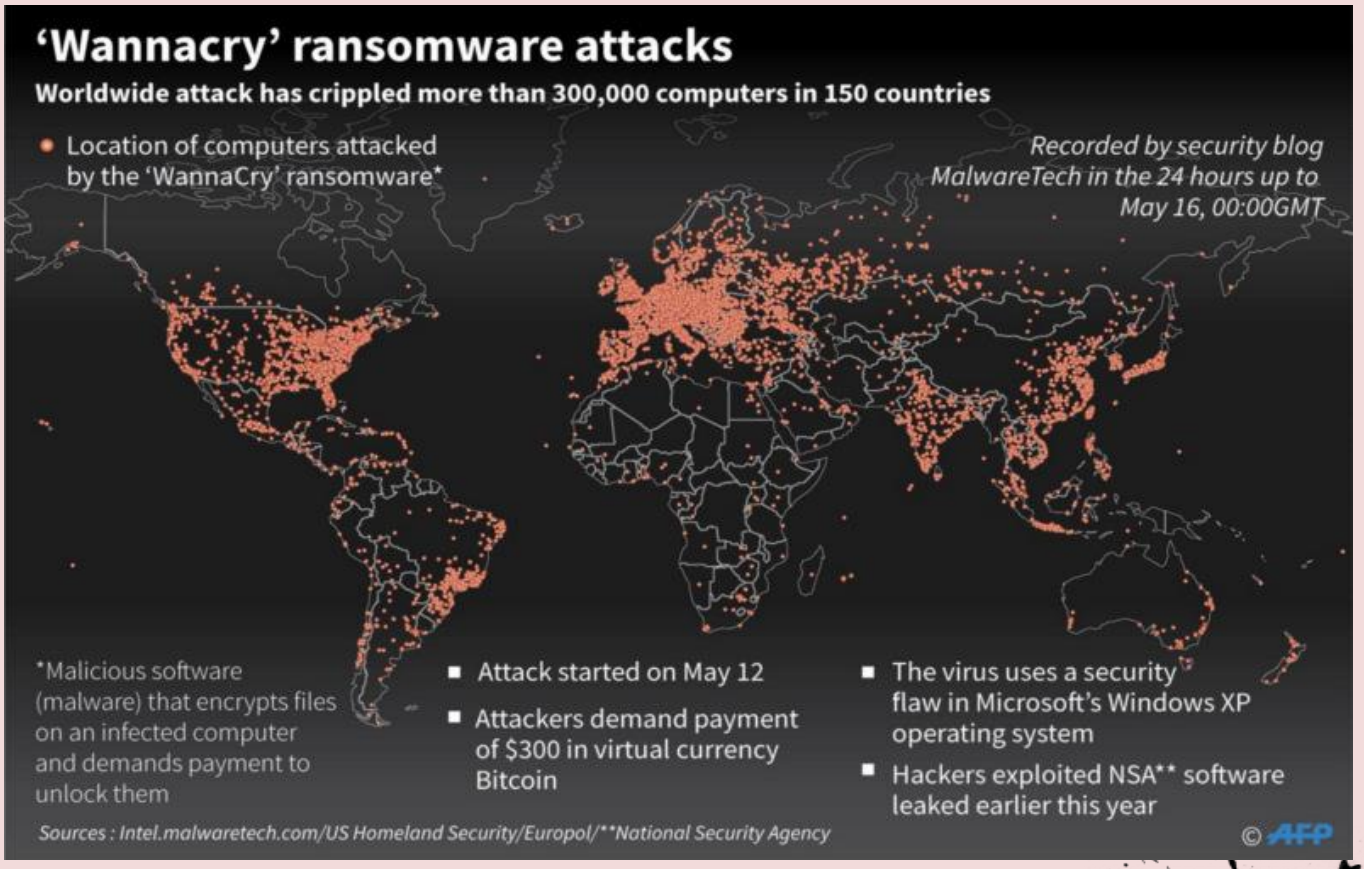
June 10 – Today's most active battlefield is not located on the ground, in the air, or on the mighty seas. It's taking place on the internet – and if you're still a non-believer, spend a few minutes with the above live map to watch a representation of cyber attacks as they happen. A full-screen version is also available. Created by Norse Corporation, a cyber intelligence firm that claims to get instant attack telemetry from over eight million sensors deployed worldwide, the map visualizes cyberwar in real-time and organizes attacks by type, origin, and target.

Predator and Prey
Who is responsible for these attacks, and who is the target?
In our few minutes of watching, the United States received nearly 70% of incoming attacks:



While we were not expecting this live visualization to literally cover every single hack worldwide, this does seem to match up with the ratio from other sources. For example, in a previous infographic on cyberwar, we noted that the U.S. is targeted in 66% of web application attacks, and in 54% of cyber espionage hacks.
In our few minutes of watching, about half of the attacks also originated from the United States. However, many also were launched from other countries such as China, Ukraine, and The Netherlands.

The Scale is Real



While the idea of cyber warfare still seems like science fiction for many people, recent events such as the WannaCry ransomware attack have made the scale and potential implications of cyber warfare much more real.

The above map from AFP shows that the WannaCry attack was unprecedented in scale, infecting more than 230,000 computers in over 150 countries. Using an exploit developed by the NSA, WannaCry infected Britain's National Health Service (NHS), Spain's Telefónica, FedEx, and Deutsche Bahn, along with many other companies or countries.
Ultimately, the hack had a built-in "killswitch" that was discovered by internet security experts. It also seemed to be relatively ineffective at collecting hefty amounts of ransom. Despite all of this, the reality is that the hack shut down hospitals and other businesses, giving us a true taste of the scale and impact that a professionally-executed cyber attack could have in the future.

Can the world ever really keep terrorists off the internet?

By Shontavia Johnson
Source: http://www.homelandsecuritynewswire.com/dr20170612-can-the-world-ever-really-keep-terrorists-off-the-internet

June 12 – After London's most recent terror attacks, British Prime Minister Theresa May called on countries to collaborate on internet regulation to prevent terrorism planning online. May criticized online spaces that allow such ideas to breed, and the companies that host them.
May did not identify any companies by name, but she could have been referring to the likes of Google, Twitter and Facebook. In the past, British lawmakers have said these companies offer terrorism a platform. She also might have been referring to smaller companies, like the developers of apps like Telegram, Signal and Wickr, which are favored by terrorist groups. These apps offer encrypted messaging services that allow users to hide communications.
May is not alone in being concerned about attacks on citizens. After her comments on Sunday, U.S. President Donald Trump vowed to work with allies and do whatever it takes to stop the spread of terrorism. He did not, however, specifically mention internet regulation.
Internet companies and other commentators, however, have pushed back against the suggestion that more government regulation is needed, saying weakening everyone's encryption poses different public dangers. Many have also questioned whether some regulation, like banning encryption, is possible at all.
Because the internet is geographically borderless, nearly any message can have a global audience. Questions about online regulation have persisted for years, especially regarding harmful information. **As a law professor who studies the impact of the internet on society, I believe the goal of international collaboration is incredibly complicated, given global history.**

Some control is possible
While no one country has control over the internet, it is a common misconception that the internet cannot be regulated. In fact, individual countries can and do exert significant control over the internet within their own borders.
In 2012, for example, the Bashar al-Assad regime shut down the internet for all of Syria. According to Akamai Technologies, an internet monitoring company, the country went entirely offline on Nov. 29, 2012. The internet blackout lasted roughly three days.
China aggressively blocks access to more than 18,000 websites, including Facebook, Google, The New York Times and YouTube. While there are some limited workarounds, the Chinese government regularly targets and eliminates them.
French courts have prohibited the display and sale of Nazi materials online in France by Yahoo's online auction service. After losing a legal case, Yahoo banned the sale of Nazi memorabilia from its website worldwide, though it denied that the move was in direct response to the court ruling.
Even in the United States, local governments have shut down mobile data and cellphone service during protests. In addition, the United States reportedly either is developing or has developed its own internet "kill switch" for times of national crisis.

International collaboration
These types of regulation efforts aren't limited to individual governments. Groups of countries

have successfully collaborated to pursue common goals online.

The Global Privacy Enforcement Network, for example, is a network of representatives from nearly 50 countries including the United States, Australia, the United Kingdom and Germany. The GPEN works to develop shared enforcement practices related to internet privacy and has reviewed many companies' online privacy policies. When the GPEN discovers websites or apps that violate a country's privacy laws, it informs the administrators or developers and encourages them to follow those laws. The group can recommend countries take enforcement action against websites or apps that do not comply.

The European Union, made up of 28 countries, has also worked to regulate harmful messages on the internet. In 2016, the European Commission announceda joint agreement with internet companies Facebook, Microsoft, Twitter and YouTube. Among other things, the companies agreed to create clear and rapid processes for reviewing potentially objectionable information and removing it if need be.

At the UN

In addition, the United Nations has been pursuing general global regulation of the internet. The U.N.'s first Working Group on Internet Governance was created in 2004 to propose models for global internet regulation. Unfortunately, the working group has not been able to agree on how to create new transnational bodies with rule-setting or regulatory power over the internet. Each country has different views on the global political issues raised by the internet's vast reach. While some countries can find common ground, it may be nearly impossible to create a worldwide model that harmonizes all of these perspectives.

The farthest the U.N. has gotten so far has been creating the Internet Governance Forum, which brings together governments, private companies and individuals to address questions about internet regulation. The group has discussed and reported on internet access, human rights and free speech issues. These discussions are an opportunity to exchange experiences and views, but there are no negotiated outcomes, rules or laws that come from the IGF.

Finding widespread common ground on internet-based issues will likely only become more difficult as the U.K. exits from the EU and the U.S. takes increasingly nationalist positions. Even so, the experiences of smaller groups of countries may inform a broader effort as global policies on terrorism shift, and the world's approach to internet regulation changes with it.

__Shontavia Johnson__ is Professor of Intellectual Property Law, Drake University.

Russia has developed a cyberweapon that can disrupt power grids, according to new research

By Ellen Nakashima

Source: https://www.washingtonpost.com/world/national-security/russia-has-developed-a-cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_story.html?utm_term=.9738b204095f

June 12 – Hackers allied with the Russian government have devised a cyberweapon that has the potential to be the most disruptive yet against electric systems that Americans depend on for daily life, according to U.S. researchers.

The malware, which researchers have dubbed **CrashOverride**, is known to have disrupted only one energy system — in Ukraine in December. In that incident, the hackers briefly shut down one-fifth of the electric power generated in Kiev.

But with modifications, it could be deployed against U.S. electric transmission and distribution systems to devastating effect, said Sergio Caltagirone, director of threat intelligence for Dragos, a cybersecurity firm that studied the malware and issued a report on Monday.

And Russian government hackers have already shown their interest in targeting U.S. energy and other utility systems, researchers said.

"It's the culmination of over a decade of theory and attack

scenarios," Caltagirone warned. "It's a game changer."

The revelation comes as the U.S. government is investigating a wide-ranging, ambitious effort by the Russian government last year to disrupt the U.S. presidential election and influence its outcome. That campaign employed a variety of methods, including hacking hundreds of political and other organizations, and leveraging social media, U.S. officials said.

Dragos has named the group that created the new malware **Electrum**, and has determined with high confidence that it used the same computer systems as the hackers who attacked the Ukraine electric grid in 2015. That attack, which left 225,000 customers without power, was carried out by Russian government hackers, other U.S. researchers concluded. U.S. government officials have not officially attributed that attack to the Russian government, but some privately say they concur with the private sector analysis.

"The same Russian group that targeted U.S. [industrial control] systems in 2014 turned out the lights in Ukraine in 2015," said John Hultquist, who analyzed both sets of incidents while at iSight Partners, a cyber-intelligence firm now owned by FireEye, where he is director of intelligence analysis. Hultquist's team had dubbed the group Sandworm.

"We believe that Sandworm is tied in some way to the Russian government — whether they're contractors or actual government officials, we're not sure," he said. "We believe they are linked to the security services."

Sandworm and Electrum may be the same group or two separate groups working within the same organization, but the forensic evidence shows they are related, said Robert M. Lee, chief executive of Dragos.

The Department of Homeland Security, which works with the owners of the nation's critical infrastructure systems, did not respond to a request for comment Sunday.

Energy-sector experts said that the new malware is cause for concern, but that the industry is seeking to develop ways to disrupt attackers who breach their systems.

"U.S. utilities have been enhancing their cybersecurity, but attacker tools like this one pose a very real risk to reliable operation of power systems," said Michael J. Assante, who worked at Idaho National Labs and is former chief security officer of the North American Electric Reliability Corporation, where he oversaw the rollout of industry cybersecurity standards.

CrashOverride is only the second instance of malware specifically tailored to disrupt or destroy industrial control systems. Stuxnet, the worm created by the United States and Israel to disrupt Iran's nuclear capability, was an advanced military-grade weapon designed to affect centrifuges that enrich uranium.

In 2015, the Russians used malware to gain access to the power supply network in western Ukraine, but it was hackers at the keyboards who remotely manipulated the control systems to cause the blackout — not the malware itself, Hultquist said.

With CrashOverride, "what is particularly alarming . . . is that it is all part of a larger framework," said Dan Gunter, a senior threat hunter for Dragos.

The malware is like a Swiss Army knife, where you flip open the tool you need, and where different tools can be added to achieve different effects, Gunter said.

Theoretically, the malware can be modified to attack different types of industrial control systems, such as water and gas. However, the adversary has not demonstrated that level of sophistication, Lee said.

Still, the attackers probably had experts and resources available not only to develop the framework but also to test it, Gunter said. "This speaks to a larger effort often associated with nation-state or highly funded team operations."

One of the most insidious tools in CrashOverride manipulates the settings on electric power control systems. It scans for critical components that operate circuit breakers and opens the circuit breakers, which stops the flow of electricity. It continues to keep them open even if a grid operator tries to close them, creating a sustained power outage.

The malware also has a "wiper" component that erases the software on the computer system that controls the circuit breakers, forcing the grid operator to revert to manual operations, which means driving to the substation to restore power.

With this malware, the attacker can target multiple locations with a "time bomb" functionality and set the malware to trigger simultaneously, Lee said. That could create outages in different areas at the same time.

The outages would last a few hours and probably not more than a couple of days, Lee said. That is because the U.S. electric industry has trained its operators to handle disruptions caused by large storms. "They're used to having to restore power with manual operations," he said.

So although the malware is "a significant leap forward in tradecraft, it's also not a doomsday scenario," he said.

The malware samples were first obtained by ESET, a Slovakian research firm, which shared some of them with Dragos. ESET has dubbed the malware Industroyer.

***Ellen Nakashima** is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.*

Stuxnet, the sequel: Dangerous malware aims to disrupt industrial control systems

Source: http://www.homelandsecuritynewswire.com/dr20170613-stuxnet-the-sequel-dangerous-malware-aims-to-disrupt-industrial-control-systems

June 13 – ESET researchers have been analyzing samples of dangerous malware (detected by ESET as Win32/Industroyer, and named **"Industroyer"**) capable of performing an attack on power supply infrastructure. The malware was likely involved in the December 2016 cyberattack on Ukraine's power grid that deprived part of its capital, Kiev, of power for over an hour.

"The recent attack on the Ukrainian power grid should serve as a wake-up call for all those responsible for the security of critical systems around the world," warns ESET Senior Malware Researcher Anton Cherepanov.

ESET researchers discovered that Industroyer is capable of directly controlling electricity substation switches and circuit breakers. It uses industrial communication protocols used worldwide in power supply infrastructure, transportation control systems, and other critical infrastructure. The potential impact may range from simply turning off power distribution, triggering a cascade of failures, to more serious damage to equipment.

"Industroyer's ability to persist in the system and to directly interfere with the operation of industrial hardware makes it the most dangerous malware threat to industrial control systems since the infamous Stuxnet, which successfully attacked Iran's nuclear program and was discovered in 2010," concludes Cherepanov.

Additional technical details on the malware and analysis can be found in an article and in a white paper on ESET's blog, WeLiveSecurity.com.

Cybersecurity experts from Imperva and Tripwire commented on the threat:

Terry Ray, chief product strategist for Imperva said:

We are beginning to see an uptick in infrastructure attacks, and in the case of Industroyer, the attackers seem to have extensive knowledge about industrial control protocols. Since the industrial controls used in the Ukraine are the same in other parts of Europe, the Middle East and Asia, we could see more of these attacks in the future. And while these attackers seem to be content to disrupt the system, it's not outside the realm of possibility that they could take things a step further and inflict damage to the systems themselves.

While ICS are used heavily in energy and water, both certainly critical infrastructure, it is also used in large scale automation, which can include, manufacturing, shipping, aerospace and other industries that should also take note of such exploits.

Many of these industrial control systems have been in operation for years with little or no modification (no anti-virus updates or patches). This leaves them open to a wide range of cyber threats. It is therefore imperative that we find alternative measures to manage the risk.

Paul Edon, director of international customer services for Tripwire said:

Historically Industrial networks have used airgap and diode based architecture to defend against the risks associated with corporate intranet and Internet communications. However, due

to economic pressures i.e. increasing costs and decreasing numbers of skilled resources, it has become necessary for many organizations to centralize some of the management and control functions that would have previously been local to industrial plants, refineries, distribution facilities etc. This centralization has meant expanding the reach of the enterprise network into the industrial environment, and in doing so, exposing those industrial environments to levels of cyber risk for which they were neither secured nor designed.

Post design security is always a much greater challenge than the "security by design and default" that we would expect today. However, the majority of attacks can still be defended against by employing the same strategy as that used for the enterprise i.e. "Security Best Practise," "Defence in Depth," and "Foundational Controls."

For Security Best Practices, select suitable frameworks such as NIST, ISO, CIS, ITIL etc. to help direct, manage and drive security programmes and ensure your strategy includes all three pillars of security; People, Process and Technology.

For defence in depth, protection should apply at all levels; Perimeter, Network and End Point. Again, make sure you are supporting your efforts using all three pillars of security; People, Process and Technology.

For Foundational Controls, select the foundational controls that best suit your environment. Firewalls, IDS/IPS, Encryption, Duel Factor Authentication, System Integrity Monitoring, Change Management, Off-line Backup, Vulnerability Management and Configuration Management to name but a few. Don't forget - ensure you are taking advantage of all three pillars of security; People, Process and Technology.

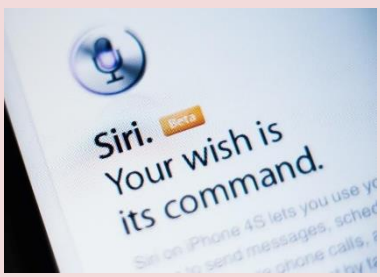
We will continue to see the introduction of new threats targeting the industrial technologies, but it is important to understand that good security hygiene will greatly reduce the effectiveness and therefore the success."

Senator Maria Cantwell (D-Washington), the top Democrat on the Energy and Natural Resources panel, told *Politico* that the malware illustrated the dangers of the fiscal 2018 budget proposed by President Donald Trump. For instance, the Trump budget proposes a reduction in funding for the Energy Department's Office of Electricity Delivery and Energy Reliability, which works to strengthen grid defenses against hackers. "Instead of responsibly performing the requested assessment that today we've discovered is more necessary than ever, the administration has proposed slashing funding to the very offices tasked with protecting our grid from Russian cyberattack," Cantwell said.

"This is where you really see the convergence of cyber and physical into destructive attacks," Caitlin Durkovich, a former assistant secretary for infrastructure protection and now a director at Toffler Associates, told *Politico*. "It is concerning." Yet she added: "We have had a very good battle rhythm and partnership between government and industry. In the last three or four years, there has been more unity of effort around the protection of the grid." She said **DHS has been, or likely would be, offering malware analysis and advice to industry and convening calls with top energy company officials. In fact, DHS's Computer Emergency Readiness Team issued an alert Monday evening.**

Preventing voice hacking

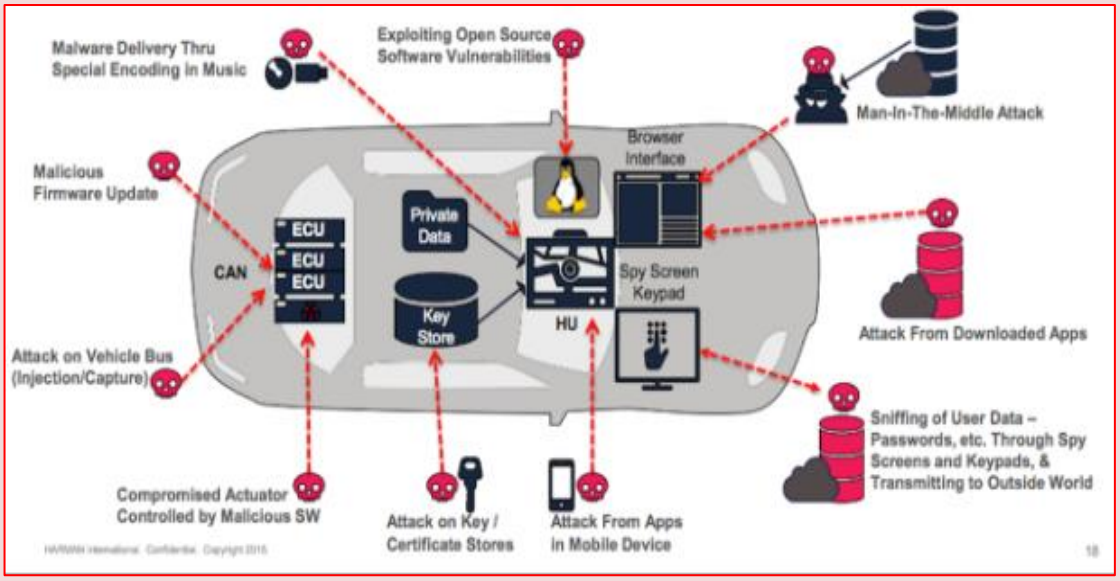
Source: http://www.homelandsecuritynewswire.com/dr20170613-preventing-voice-hacking



June 13 – While convenient, Siri, WeChat, and other voice-based smartphone apps can expose you to a growing security threat: voice hacking. With just a few minutes of audio samples, attackers can replay your voice convincingly enough to trick people as well as top digital security systems. The consequences, from impersonating you with your friends to dipping into your bank account, are terrifying. An app, soon to be available, will help thwart growing cybersecurity threat.

Preventing autonomous vehicles from being hacked

Source: http://www.homelandsecuritynewswire.com/dr20170613-preventing-autonomous-vehicles-from-being-hacked



June 13 – Although autonomous vehicles are essentially large computers on wheels, securing them is not the same as securing a communication network that connects desktop computers and smartphones to large geographical areas due to the roles that the sensors and actuators play in the physical layer of the network. Researchers have developed an intelligent transportation system prototype designed to avoid collisions and prevent hacking of autonomous vehicles.

How a cyber attack transformed Estonia

Source: http://www.bbc.com/news/39655415

It all began when Estonian authorities decided to move a memorial to the Soviet Red Army to a position of less prominence in the capital, Tallinn

Apr 27 – Cyber-attacks, information warfare, fake news - exactly 10 years ago Estonia was one of the first countries to come under attack from this modern form of hybrid warfare.
It is an event that still shapes the country today.
Head bowed, one fist clenched and wearing a World War Two Red Army uniform, the Bronze Soldier stands solemnly in a quiet corner of a cemetery on the edge of the Estonian capital Tallinn.

Flowers have been laid recently at his feet. It is a peaceful and dignified scene. But in April 2007 a row over this statue sparked the first known cyber-attack on an entire country.
The attack showed how easily a hostile state can exploit potential tensions within another society. But it has also helped make Estonia a cyber security hotshot today.

From outrage to outage

Unveiled by the Soviet authorities in 1947, the Bronze Soldier was originally called "Monument to the Liberators of Tallinn". For Russian speakers in Estonia he represents the USSR's victory over Nazism.

But for ethnic Estonians, Red Army soldiers were not liberators. They are seen as occupiers, and the Bronze Solider is a painful symbol of half a century of Soviet oppression.
In 2007 the Estonian government decided to move the Bronze Soldier from the centre of Tallinn to a military cemetery on the outskirts of the city.
The decision sparked outrage in Russian-language media and Russian speakers took to the streets. Protests were exacerbated by false Russian news reports claiming that the statue, and nearby Soviet war graves, were being destroyed.
On 26 April 2007 Tallinn erupted into two nights of riots and looting. 156 people were injured, one person died and 1,000 people were detained.
From 27 April, Estonia was also hit by major cyber-attacks which in some cases lasted weeks.
Online services of Estonian banks, media outlets and government bodies were taken down by unprecedented levels of internet traffic. Massive waves of spam were sent by botnets and huge amounts of automated online requests swamped servers.
The result for Estonians citizens was that cash machines and online banking services were sporadically out of action; government employees were unable to communicate with each other on email; and newspapers and broadcasters suddenly found they couldn't deliver the news.
Liisa Past was running the op-ed desk of one of Estonia's national newspapers at the time, and remembers how journalists were suddenly unable to upload articles to be printed in time. Today she is a cyber-defence expert at Estonia's state Information System Authority.
"Cyber aggression is very different to kinetic warfare," she explained. "It allows you to create confusion, while staying well below the level of an armed attack. Such attacks are not specific to tensions between the West and Russia. All modern societies are vulnerable."
That means that a hostile country can create disturbance and instability in a Nato country like Estonia, without fear of military retaliation from Nato allies.

Shadowy forces

The alliance's Article Five guarantees that Nato members defend each other, even if that attack is in cyberspace. But Article Five would only be triggered if a cyber-attack results in major loss of life equivalent to traditional military action.
Identifying who is responsible also makes retaliation difficult. The 2007 attacks came from Russian IP addresses, online instructions were in the Russian language and Estonian appeals to Moscow for help were ignored.
But there is no concrete evidence that these attacks were actually carried out by the Russian government.
On condition of anonymity, an Estonian government official told the BBC that evidence suggested the attack "was orchestrated by the Kremlin, and malicious gangs then seized the opportunity to join in and do their own bit to attack Estonia".
Hostile states often count on copycat hackers, criminal groups

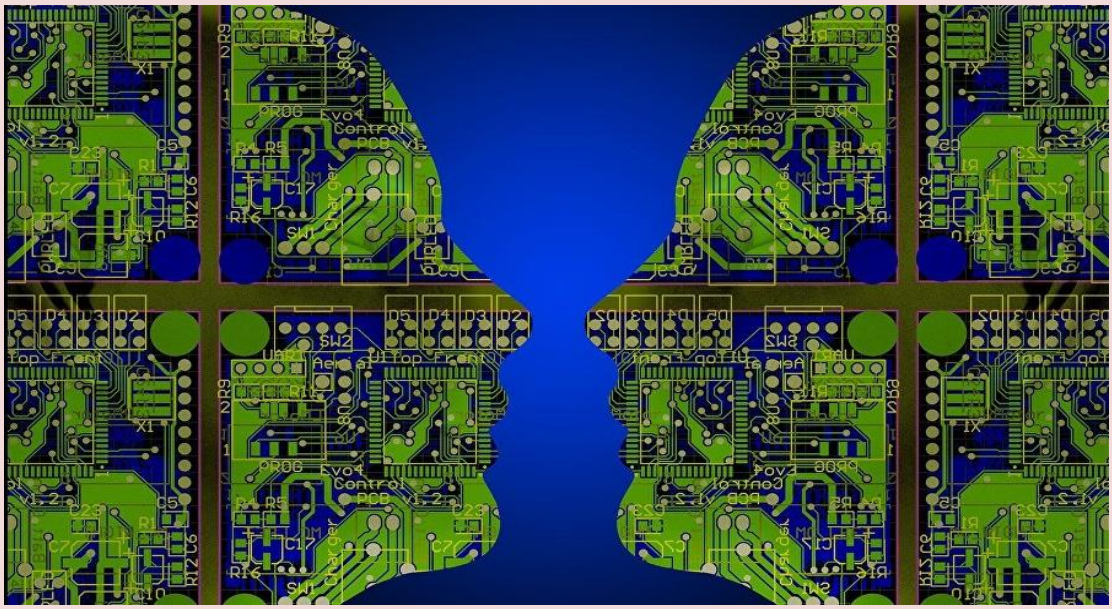
and freelance political actors jumping on the bandwagon.
2007 was a wake-up call, helping Estonians become experts in cyber defence today. "It was a great security test. We just don't know who to send the bill to," says Tanel Sepp, a cyber security official at Estonia's Ministry of Defence.
The Bronze Soldier attacks may be the first suspected state-backed cyber-attacks on another nation.
But since then cyber warfare has been used all over the world, including in Russia's war with Georgia in 2008, and in Ukraine. "Cyber has become a really serious tool in disrupting society for military purposes," says Tanel Sepp.
That's why Estonia's government has now set up a voluntary Cyber Defence Unit. Since Russia's 2014 annexation of Crimea, the Estonian Defence League has been much reported on by the international press: at weekends 25,000 volunteers don fatigues and head to the forests to learn how to shoot.
Less well known is the shadowy Cyber Defence Unit.

Once bitten

The country's leading IT experts are also trained by the Ministry of Defence. But in addition they are security vetted and remain anonymous.
They donate their free time to defending their country online by practising what to do if a major utility or vital service provider is brought down by a cyber-attack.
It's the sort of private sector talent the state could never usually afford to employ.
But the memory of 2007 is a good recruiting sergeant. The attacks have stuck in the national consciousness by proving to Estonians the importance of cyber security.
Ten years after the attacks, the Bronze Soldier is still a reminder how much Estonia's complicated past can disrupt the present.

Forget Atomic Bomb, Here's What Could Become the Next Super Weapon

Source: https://sputniknews.com/science/201706191054763840-possibly-next-super-weapon/



June 19 – **The new super weapon of the 21st century will not be an atomic or thermonuclear bomb, but self-learning artificial intelligence systems,** which are already being developed by the world's leading powers, according to French futurist Jean-Christophe Bonn.
During a press conference in Kaspersky Lab, dedicated to the festival "Kaspersky Geek Picnic," Bonn said that Nelson Mandela wrote in 1995 that the main weapon of the 21st century would be education and that it would replace nuclear weapons and other weapons of mass destruction of the 20th century.
"To me it seems that it will be artificial intelligence systems. For their function, unlike an atomic

bomb, there is no need for uranium, or factories or other hard-to-reach materials. Only silicon and electricity are needed," the French researcher said.

Talking about what makes artificial intelligence (AI) a super weapon, the scientist said that the creation and development of artificial intelligence systems couldn't be traced.

The International Atomic Energy Agency (IAEA) and other nuclear departments can trace signs of uranium, plutonium and other radionuclides next to secret objects, say in North Korea or Iran but they cannot trace AI.

Therefore, the emergence of such a "super weapon" will be extremely difficult or even impossible to predict.

"Politicians and representatives of the security agencies of France, Israel and many other countries deny that they are developing similar systems for conducting cyber war. Is that really so, we cannot check. But, it seems to me, these developments are being carried out and this is the main strategic task for most leading powers," Bonn said.

If such a powerful weapon could already be created, what would stop countries from using it?

According to Anton Shingarev, vice president of Kaspersky Lab, the NATO countries consider cyber attacks equivalent to physical attacks and reserve the right to respond to such a threat in any way they want.

In addition, cyber weapons will make attackers vulnerable also because today's modern industrial and military facilities use similar equipment, operating according to similar principles and are connected to the same global network.

Accordingly, the victim of a cyber attack can analyze and respond in a similar way. For now, at least, that makes such attacks at a state level quite meaningless.

Soteria Intelligence Develops AI-Powered Counter-Terrorism Solution, Expands Focus on Marketing/PR Industry

Source: http://www.soteriaintelligence.com/

June 20 – Soteria Intelligence is excited to announce that after four years of research and development the company's proprietary artificial intelligence platform aimed at combating terrorism has come to life. Additionally, AI-powered social media intelligence solutions for brand reputation management and public relations are now available.

Soteria Intelligence set out to build revolutionary technologies with the power to counter evil by using a blend of machine learning, including image recognition and language processing, as well as proprietary historical data, algorithms, input from subject-matter experts, and more. The robust platform is one of many announcements the company will be making in the near future.

"A big focus for us was to approach counter-terrorism by looking at what people actually say or do that could be cause for concern instead of relying on basic metrics, such as combinations of keywords or simple searches that often result in profiling based on race, color, religion, etc.," stated Aaron Schoenberger, Founder and CEO of Soteria Intelligence. The company realized AI was the only way to solve a big data problem of this kind, and to do so in an effective, non-biased manner with the ultimate goal of saving lives – all lives.

Soteria Intelligence has also used its social media expertise and artificial intelligence capabilities to create solutions specifically geared towards extracting actionable intelligence

from social networks, which will empower organizations. Use cases range from detecting/countering emerging PR catastrophes to threats on social media that can disrupt operations, damage brand reputation or affect stock prices.

By tapping AI, Soteria Intelligence is able to cut through the noise, find needles in digital haystacks, and eliminate false positives, thus providing truly intelligent insights.

For example, having the ability to automatically tell the difference between "I am going to bomb X after this croissant" versus "I had a bomb croissant at X." Similar words, totally different meanings.

Terrorism 3.0, London Blowback Raise New Issues

By Oz Sultan

Source: http://www.newsmax.com/OzSultan/terrorism-london-nabra-hassanen/2017/06/20/id/797087/

June 20 – Over the past several decades, we have seen an ebb and flow of responses

stemming from military incursions and the reprisals of terrorists, the world over. Such was the nature of war, as nation states were well defined and enemies understood within the borders of faraway lands.

Blowback used to be understood solely as the response of a terrorist or state actor group against another — however the understanding of this has changed recently.

The rise of ISIS and their prolonged guerilla siege of cities across the globe has changed the nature of terrorism — leading to the current state we call Terrorism 3.0. This is a world where ISIS has spread to approximately 37 countries. Terrorism has become syndicated and is developing by partnership, such as Waliyat Khurasan being designated ISIS-K in Iraq and the rise of ISIS associations with Abu Sayyaf, in the Philippines.

This rise has been punctuated by attacks across the globe from the Middle East to Europe, Asia and America. As police and intelligence agencies are looked to as the protectors of domestic economies, we have seen that they are often woefully incompetent or ill-prepared to tackle the challenge that Terrorism 3.0 or de-centralized, non-state-actor terrorism presents. The U.K. and France emblematic of this with the Manchester and London attacks presenting terrorist actors that were referred to intelligence or police counterterrorism departments numerous times previously; while Paris attack after Paris attack evidences the results of studies showing limited coordination and problems with information sharing, coordination, and remediation. In the U.S., while intelligence and the successful integration of American Muslims has led to fewer attacks, there are still intelligence gaps that should be solved by augmenting failed CVE (Countering Violent Extremism) programs with public-private partnerships that engage Muslim communities — which has been proven a better path and is a lesson that the EU should consider implementing.

What terror attacks have done is effectively marginalize Muslim communities — while strangling them with the yoke of collective culpability. This has resulted in attacks in the past — but not wholescale blowback.

While fringe attacks on American Muslims and European Muslims have been studied within Counterterrorism and Civil Rights arenas for years — we didn't have clearly defined cases of blowback until this week. In the U.K., a 47-year-old father of four, Darren Osborne, rented a van approximately 12 miles from his home in Cardiff and drove over 150 miles to London, where he mowed down British Muslim worshippers, killing one and injuring 11. In Virginia, an eerie parallel could be drawn to the brutal murder of Nabra Hassanen — who was kidnapped and bludgeoned to death by Darwin Martinez Torres.

What classifies both of these cases as blowback or potential blowback is the nature and severity of the attack. In the U.K., copycatting an

attack method used by ISIS and in the U.S. — an argument between a driver and a group of young American Muslim girls leading to kidnapping and murder over a period of 24 hours.

What these cases raise is a new arena of risk for both law enforcement and intelligence gathering organizations. Terrorism is seen as something that tries to change the way of life as we know it — however with the rise of blowback and potential blowback, we need to be crunching data and assessing risk profiling. **We also need to start moving from antiquated Terrorism 2.0 profiling methods to Terrorism 3.0 data driven analysis.** This analysis could lead to better indicators of risk and better methods of preventing domestic terror from blowback responses. Further, we should be focusing on public-private partnerships with Muslim communities to leverage them as partners and a first line of defense. Technology also needs to play a part in fixing the information silos within law enforcement organizations — because beyond the need for a new approaches, preventing terror ultimately prevents blowback.

__Oz Sultan__ is a leading Big Data and counterterrorism expert who focuses on anti-recruiting and ISIS counterterror (CT) research within social media. He is an advisor to the Center for the Study of Civil Military Operations at Westpoint and is adjunct faculty at CUNY Baruch.

Virtual Reality Police Training on The Move

Source: http://i-hls.com/archives/77110?mc_cid=4b1b5c74f6&mc_eid=521c0e089a

June 18 – Singapore police have been testing a new mobile virtual reality (VR) training classroom for its officers. Inside and across the length of the soundproofed truck are two wide virtual reality panels. Two pairs of police officers can be put to the test in up to seven random scenarios, such as a gunman at a coffee shop or a domestic fight that quickly escalates into a knife attack. Two of the scenarios are terrorism-related.

The training solution was devised over six months by the Home Team Academy, with the Office of the Chief Science and Technology Officer and the Singapore Police Force.

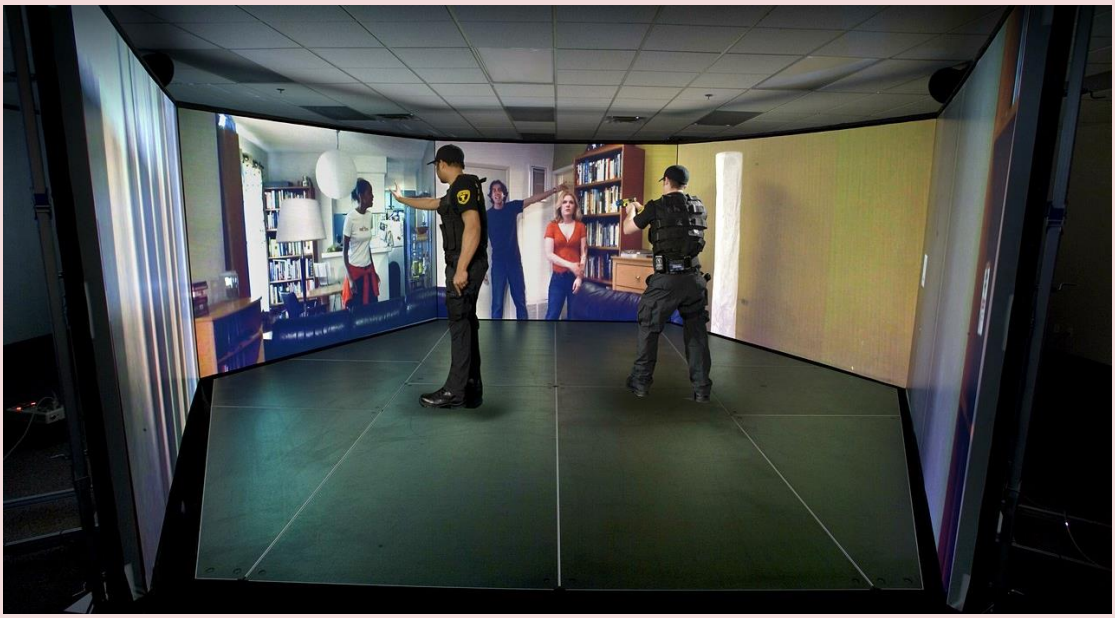
The prototype truck will travel to the six police land divisions across Singapore for a six-month trial to train police personnel.

Controlling the screen using VR-enabled weapons — which can be a revolver, a taser or a baton — the officers will be evaluated on their choice of weapon in response to the sudden incident, according to todayonline.com.

Their reaction times will also be clocked, and how they use verbal commands to try to control the situation will be reviewed through a video playback system.

The truck also stores another platform that can be laid out in a space no larger than half a badminton court. It includes four collapsible virtualizers omnidirectional treadmills allowing

users to move in a virtual world, so that more officers can concurrently undergo the same test as those on the truck.



The mobile classroom, which can be sent to any neighbourhood police centre, can train up to 16 officers at a time. This can be done in 15 minutes between their shift changes, to minimise operational downtime while ramping up training frequency. It cuts down the need to rely on yearly refresher courses as well.

Ground response force officer Anderitte Lim, 22, who started training with the VR system three weeks ago, said he felt "the same stress and nerves" as he would on the ground.

He added that "it is not every day that domestic disputes turn violent", but when this VR training is done before they begin their shifts, the scenarios remain fresh in their heads, "so we will know what to do on the spot".

Home Team Academy's chief executive T Raja Kumar said that the scenario-based VR training "hones instincts and judgment" and encourages officers to articulate why they made a certain decision over another, improving team coordination.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
EMERGENCY
RESPONSE

How Would Long Island be Evacuated in an Emergency?

Source: http://www.govtech.com/em/disaster/How-Would-Long-Island-be-Evacuated-in-an-Emergency.html

May 26 – How would Long Island be evacuated in an emergency?

The short answer: There is no formal plan. Officials have ideas and tactics that work on a smaller scale, but it is logistically complicated.

The long answer: Between traffic on the Long Island Expressway, bridge construction and signal troubles on the Long Island Rail Road, there's no shortage of headache-inducing obstacles in trying to get off the Island.

But what if there were an emergency requiring evacuation?

As it turns out, evacuation tactics are pretty standard no matter where you are, said Craig Craft, commissioner of Nassau County's Office of Emergency Management. And the tactics deployed are going to depend on the emergency.

"We'd have to pull the plug and make that decision days in advance," he said.

Contraflow, the practice of **shifting highways so all lanes move in the same direction** would be a good option for an event such as superstorm Sandy, he said.

Another option, though not very efficient, would be to **use ferries to move people** across the Long Island Sound.

But even a storm like Sandy wasn't enough to require evacuating the whole Island.

"What would be a reason that we would consider an evacuation of that magnitude? Maybe a Category 5 hurricane?" Craft said. "I could see us moving people to the center of the Island and taking over a lot of areas in the center as shelters."

In the event of a terror attack or catastrophe that affects power or air quality, Craft said, officials would tell the public to shelter in place.

Part of the difficulty in coming up with a comprehensive evacuation plan is dealing with the size of the local population, officials said.

Long Island **boasts about 3 million residents** across Nassau and Suffolk counties, according to U.S. Census records. However, any event that requires an evacuation of Long Island would also likely affect New York City and its dense boroughs, which 8.5 million people call home.

So to move **more than 11 million people**, it would have to be a true emergency with lots of coordination, Craft said, and that definition is hard to pin down.

Fears about a lack of an evacuation plan helped doom the roughly $6 billion Shoreham Nuclear Power Plant, which was officially decommissioned in 1994 after two decades of controversy over its safety.
In 1983, the Suffolk County Legislature determined the county could not safely and effectively evacuate its residents in the event of a nuclear disaster, marking the project's decline.
Of course, people can always choose to self-evacuate. For some, a transportation breakdown could be enough to leave, said Chris Dowhie, owner of **Plan B Marine**. Plan B allows wealthy clients in Manhattan

to purchase a very specific type of insurance policy — access to quick, safe water transport to the mainland.
Clients pay as much as $750 a month per person to have a private escape boat available. Plan B staff have trained clients on how to use the twin-engine, military-grade boats for the three-minute ride to New Jersey from Manhattan's West Side and Dowhie said clients include diplomats, investment advisers and college students with concerned parents.
"Mass transit, power failure, any kind of event that's going to delay you more than three, four hours from your commute," Dowhie said. "It doesn't have to be a 911 scenario or zombie apocalypse, it could be a generic inconvenience."
The bottom line is that while you may want to leave Manhattan or Long Island, there's little chance everyone will be asked to.
"There's a lot of options out there, but the likelihood of doing an island evacuation is very slim," Craft said.

Knowing more and loosing less: Science and helps in disaster risk management

Source: http://www.homelandsecuritynewswire.com/dr20170529-knowing-more-and-loosing-less-science-and-helps-in-disaster-risk-management

May 29 – Natural and man-made disasters threaten millions of people every year and cause billions of property damage. How much do we know about them? And how can we use that knowledge to save lives and money? A recent report, compiled by the European Commission's Science and Knowledge Service (JRC), seeks to answer these and other questions and to help prepare for the time when disaster strikes. The report, Science for Disaster Risk Management 2017: Knowing More and Losing Less, is a product of the European Commission's Disaster Risk Management Knowledge Centre (DRMKC). It presents the state-of-the-art in disaster risk management. The EC says that the report contributes to UN efforts to strengthen prevention, preparedness, and response to calamities and it is also a key part of the Science and Technology Roadmap of the Sendai Framework for Disaster Risk Reduction. The report was presented last week at the UN Global Platform for Disaster Risk Reduction in Cancun.

What role for science in managing disasters

Science plays a key role in preventing disasters, preparing for the ones that cannot be prevented and recovering from them. Using already existing knowledge more widely would save the lives and livelihoods of millions of people around the world. The report contributes to this objective by presenting the best available knowledge in various fields of Disaster Risk Management, such as risk assessment and risk communication, across the whole spectrum of hazards (earthquakes, tsunami, floods, extreme weather, epidemics, nuclear and chemical accidents, etc.) and throughout the entire disaster risk management cycle.

What do we know and what can we do more

The report also highlights knowledge gaps and identifies needs for further research in order better to understand disasters and improve the effectiveness of our responses, for instance the application of internet of things in this field. The Disaster Risk Management Report analyses areas in which science and knowledge can be further integrated into policy, one example being more interoperability through development of common standards and risk assessment methods. It also identifies public Private Partnerships for risk-sharing as an area of potential improvement that when addressed can save more lives, minimize damage and improve resilience.

Background

The EC notes that the European Commission's Disaster Risk Management Knowledge Center was launched only six months after the Sendai Framework for Disaster Risk Reduction 2015-2030 was set up. The report Science for Disaster Risk Management 2017: Knowing More and Loosing Less is based on the contributions of 273 scientists from 26 countries and 172 organizations and was made possible through the collaboration between 11 services of the European Commission.

Last week in Cancun, at the UN Global Platform for Disaster Risk Reduction, the JRC also presented the Atlas of the Human Planet 2017, a comprehensive study of global population exposure to natural hazards, spreading over the last forty years.

Project "Hero": Land Rover and Red Cross

Source (video): https://www.landrover.com/experiences/news/project-hero.html

Jaguar Land Rover Special Vehicle Operations (SVO) has designed and engineered a bespoke version of the new Land Rover Discovery for use by the Austrian Red Cross.

'Project Hero' was presented to the world's media for the first time at the Geneva Motor Show.
Project Hero is an advanced communication vehicle, created to support Jaguar Land Rover's partnership with the International Federation of Red Cross and Red Crescent Societies (IFRC), the world's largest humanitarian network. SVO collaborated with the Austrian Red Cross to develop a unique Land Rover that will be trialled by their emergency response teams. It is hoped it will help the Red Cross save lives by speeding up response times to disasters.

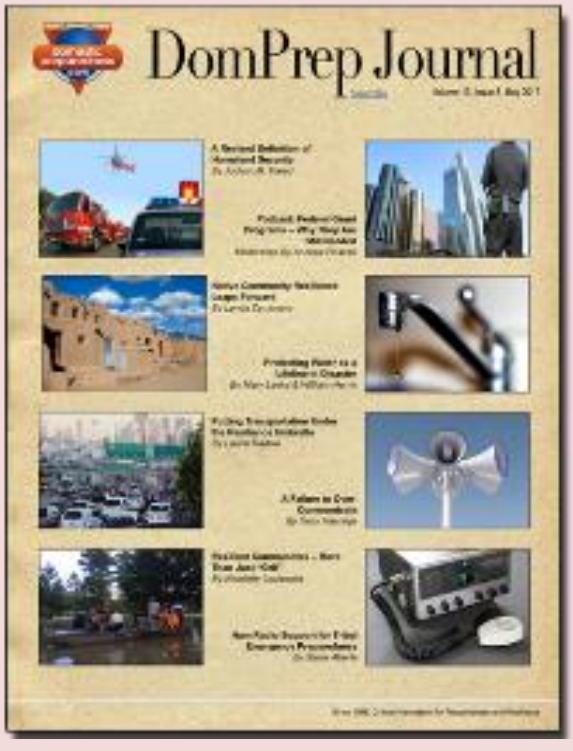
Land Rover has supported the Red Cross since 1954 and supplied 120 vehicles to the IFRC for deployment in all corners of the globe. Project Hero is the first with a roof-mounted drone. A fully integrated landing system featuring self-centring and magnetic retention technology is a world-first that enables the drone to land on Project Hero when the vehicle is in motion.
The drone enhances New Discovery's already outstanding capability. With the drone airborne, live footage can be transmitted to the Red Cross's emergency response teams, helping them respond more quickly and effectively to landslides, earthquakes, floods and avalanches. Dramatic landscape changes can make maps redundant, which adds to the danger and difficulty of finding and rescuing survivors, so the drone's bird's-eye view will allow rescuers to investigate an emergency scene from a safe distance.
John Edwards, Jaguar Land Rover Special Operations Managing Director, said: "Land Rover and the team of engineers and designers at SVO are proud to support the incredible humanitarian work of the IFRC and its members.
"The new Discovery is an outstanding all-terrain SUV, and Project Hero is the optimum combination of enhanced capability and innovative technology. We hope to help the Red Cross save lives in emergency situations."
Dr Jemilah Mahmood, IFRC Under Secretary General for Partnerships, said: "We are grateful to Land Rover for their generous support over the past 60 years, and are proud of our ambitious global partnership that has transformed the lives of millions of people on four continents.
"The partnership is supporting communities around the world to become more resilient in the face of natural disasters such as monsoons, flooding and earthquakes.
"Project Hero combines the best expertise of the Red Cross and Jaguar Land Rover to create a truly unique vehicle, which we hope will be capable of making a difference to rescue operations in the toughest environments."

Project Hero is based on the 3.0-litre TD6 engine-powered version of the new Land Rover Discovery. In

addition to the unique drone technology supplied in Project Hero, the rear of the interior in this special vehicle also features:

- Heavy-duty sliding floor in the rear load space, which may be deployed as an addition work surface, or to protect the load carried underneath
- Segregation panel behind the rear seats providing additional equipment mounting points
- Strategically positioned LED lighting to aid night vision
- Innovative power supply points which accept multiple plug arrangements from different regions

Project Hero is also equipped with multiple frequency radio equipment enabling contact to be made in a variety of situations.



Project Hero will be based at the Austrian Red Cross training centre in Erzberg, in the mountainous Eisenerz mining area, and in Vienna, for 12 months from June 2017. The drone will be used in simulations to develop new and innovative techniques for disaster relief and on test-runs for complex natural disaster scenarios, including at night and in dense forests. Project Hero will also be used when the Red Cross provides emergency support at times of natural disasters, such as heavy snow or floods, or accidents.

DomPrep Journal

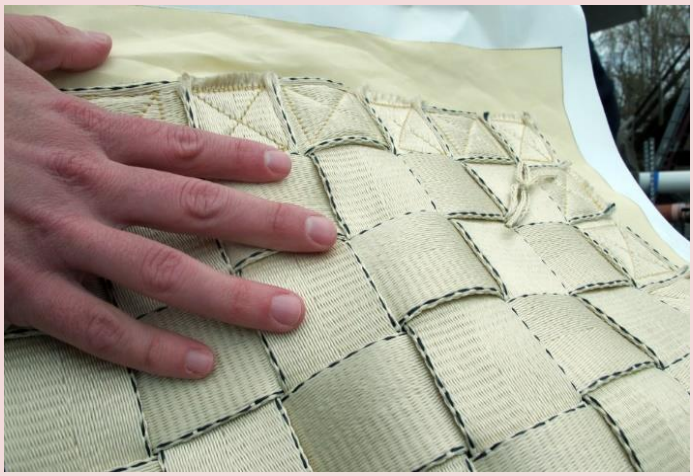
Inflatable plug for subway tunnels demonstrated

Source: http://www.homelandsecuritynewswire.com/dr20170616-inflatable-plug-for-subway-tunnels-demonstrated

June 16 – A giant, inflatable structure designed to prevent flooding in subways was rolled out, literally, for media observers inside a full-scale, mock subway tunnel. As the video shows, in under five minutes it is nearly filled with pressurized air — creating a flexible but extremely strong barrier**. Full inflation is complete in less than twelve minutes.** The live demonstration continued with the plug holding back

simulated floodwater at 11.5 pounds per square inch pushing against it.

The Department of Energy's Pacific Northwest National Laboratory helped develop the Resilient Tunnel Plug in partnership with ILC Dover and West Virginia University for the Department of Homeland Security's Science and Technology Directorate. It's kind of like a large balloon, but infinitely stronger.



"This is one of those things where we had an idea that was pretty simple but we needed to take that concept to reality," PNNL engineer Greg Holter said. "The big problem wasn't just designing the plug, but ensuring it could be stored without interfering with trains passing through their tunnels."

PNNL says that the RTP, made from a liquid crystal polymer called Vectran, was developed to provide security to transit systems as protection from flooding, primarily in subways, in the event of a terrorist attack or natural disaster. In the event of flooding, the plug would rapidly inflate, holding back a tunnel full of floodwater, keeping citizens and the transit system assets safe.

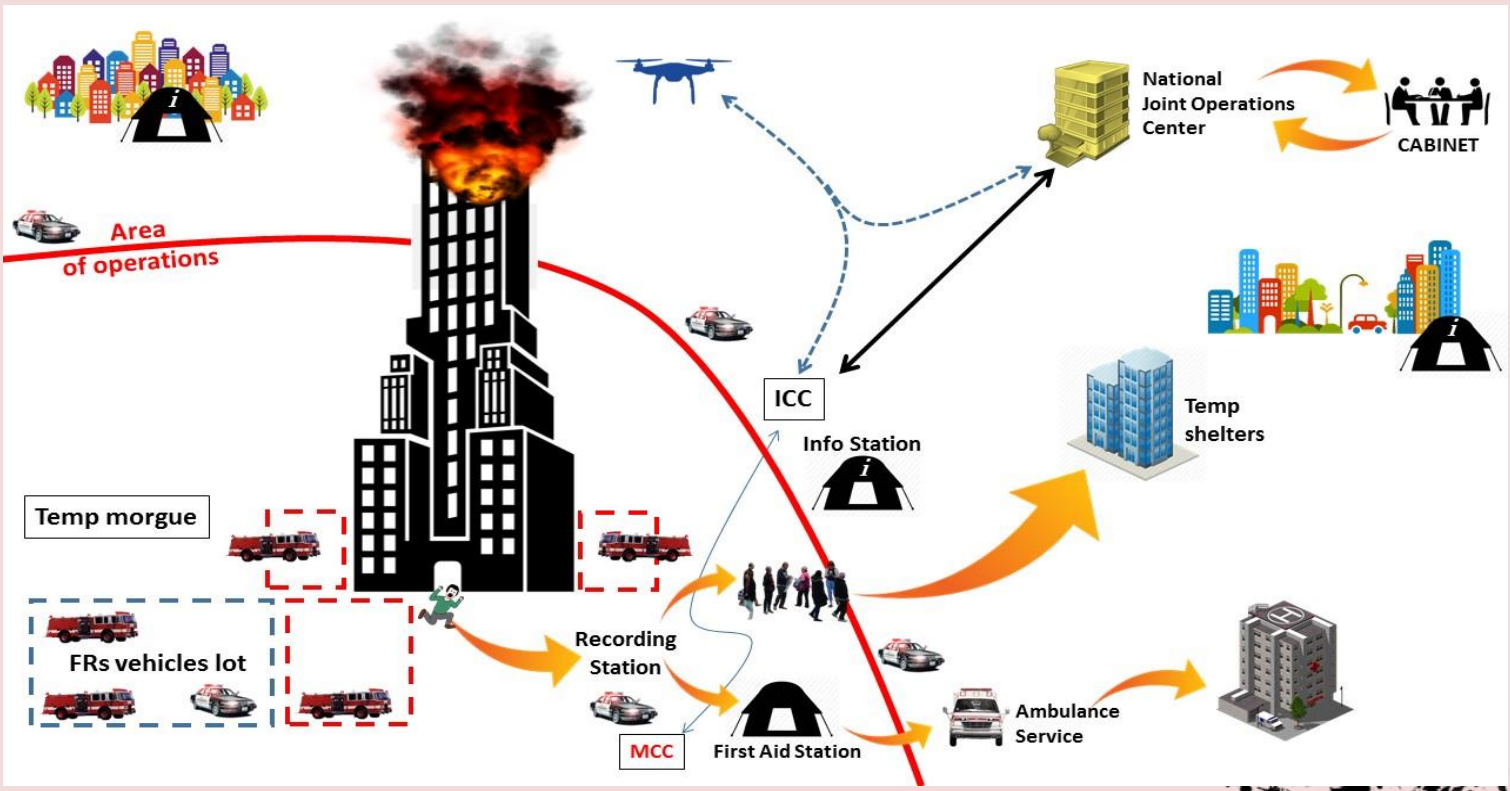
High building fire operational plan

Simple but complex

By the Editor of the CBRNE-T NSL

In modern cities there are many high building that serve either offices or appartments. It would be clever for each and every high building to have a specific response plan with all the details in one file that is

updated twice a year. This is a hard work to do but one day might pay back by saving people. Improvisations in emergencies is not the best to anticipate and during the chaotic environment that is created by all parts involved, many things might go wrong or just forgotten.
A simple (but not simplistic) approach is presented below:



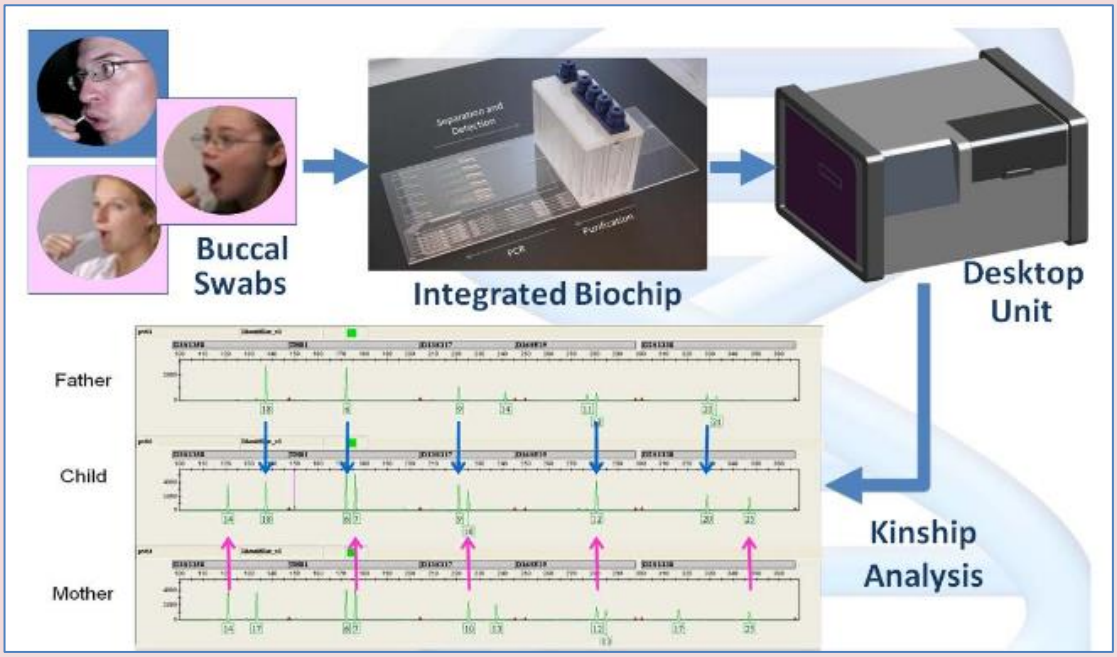
ICC = Incident Command Center; MCC = Medical Command Center; FRs = First Responders

Rapid DNA technology verifies relationships after mass casualty events

Source: http://www.homelandsecuritynewswire.com/dr20170619-rapid-dna-technology-verifies-relationships-after-mass-casualty-events

June 19 – **Rapid DNA technology developed by the Department of Homeland Security Science and Technology Directorate (S&T) has recently been used to identify simulated "victims" in several mass casualty exercises across the United States.** The technology greatly expedites the testing of deoxyribonucleic acid (DNA), the only biometric that can accurately verify family relationships. With results available in ninety minutes or less, S&T's Rapid DNA technology can be used on the scene of mass fatality events, in refugee camps around the world, or at immigration offices.

"Rapid DNA dramatically reduces the time it takes to reunify families and mass-casualty victims. What took days to several weeks (due to delays caused by shipping DNA samples to regional laboratories for testing) can now be accomplished in hours, onsite," explained Christopher Miles, S&T's Deputy Director for Standards Integration and Application.



S&T says that the technology, originally developed in partnership with the Department of Justice and the Department of Defense, was commercialized by S&T in 2015 and is now actively working to transition it to other DHS components, including Customs and Border Protection and Immigrations and Customs Enforcement, as well as other federal, state and local government organizations. The technology can support efforts in immigration, human trafficking prevention, reunification of family members following mass casualties, and DHS law enforcement investigations.

The Rapid DNA technology was put to the test in early May during a full-scale, mass-fatality exercise at locations around Dayton, Ohio. S&T's Capability Development Support (CDS) Office of Standards (STN) joined the Ohio Department of Health, Ohio National Guard, Ohio Emergency Management Agency, Montgomery County Sheriff's Office, Dayton & Montgomery County Public Health, Miami Valley Hospital and other local and state response agencies in the exercise, where the technology was used to confirm that DNA placed at the disaster sites matched the DNA of family members.

This exercise simulated local, state and federal responses to a mass fatality incident, including emergency and public health responders and mass fatality and mortuary assistance, which support and coordinate efforts to mitigate the impact of these incidents. Miles and a team of Rapid DNA operators brought Rapid DNA equipment to the exercise.

"The Rapid DNA equipment proved valuable, both as a technical tool and a way to help families handle a situation most would find unimaginably stressful," said Miles.

In preparation for the exercise, a Rapid DNA team brought two Rapid DNA instruments for demonstration at the Montgomery County Crime Laboratory, which provided blood samples, Flinders Technology Associates DNA collector paper and cheek swabs (buccal swabs) of DNA laboratory staff. The Rapid DNA team ran eleven1 samples in two hours and received results sufficient to identify the persons in 10 of those samples. The remaining blood sample had too much blood on the swab, which saturated that particular result.

The simulation began with an announcement of a gas explosion and partial structural collapse that trapped 300 persons in rubble and caused many fatalities. As local fire and emergency services put out the fire and began moving victims to local hospitals, the medical surge rapidly exceeded local healthcare capabilities

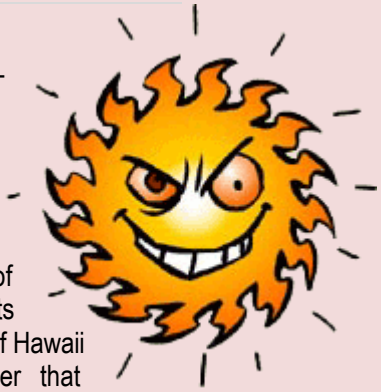
During the exercise, the Rapid DNA team demonstrated that DNA results can be obtained before the deceased are sent to storage and before family members leave family assistance centers. This process ensures good DNA samples are collected in a timely manner, families are reunited quickly and morgue and family assistance center operations are closed down as rapidly as possible. Rapid DNA saves time and money during mass fatality operations.

In late May, the technology was used at another mass casualty exercise in Florida. Miles said that both exercises used mobile morgues and family information centers as parts of their scenarios, an important aspect when reacting to disaster situations with heavy loss of life.

"We are demonstrating that DNA collected from victims at the morgue can be matched to family members that report to the family information center. DNA is the only biometric that verifies that family members are biologically related," Miles explained. "Rapid DNA is fast enough that results can be obtained before family members leave or before human remains are sent off to storage."

Deadly heatwaves on the rise

Source: http://www.homelandsecuritynewswire.com/dr20170622-deadly-heatwaves-on-the-rise



June 22 – **Seventy-four percent of the world's population will be exposed to deadly heatwaves by 2100 if carbon gas emissions continue to rise at current rates, according to a study published in *Nature Climate Change*. Even if emissions are aggressively reduced, the percent of the world's human population affected is expected to reach 48 percent.**

"We are running out of choices for the future," said Camilo Mora, associate professor of geography in the College of Social Sciences at the University of Hawaii at Manoa and lead author of the study. "For heatwaves, our options are now between bad or terrible. Many people around the world are already paying the ultimate price of heatwaves, and while models suggest that this is likely to continue, it could be much worse if emissions are not considerably reduced. The human body can only function within a narrow range of core body temperatures around 37°C. Heatwaves pose a considerable risk to human life because hot weather, aggravated with high humidity, can raise body temperature, leading to life threatening conditions."

University of Hawaii at Manoa says that a team of researchers lead by Mora conducted an extensive review and found **over 1,900 cases of locations worldwide where high ambient temperatures have killed people since 1980.** By analyzing the climatic conditions of 783 lethal heat episodes for which dates were obtained, researchers identified a threshold beyond which temperatures and humidities become deadly. The area of the planet where such a threshold is crossed for twenty or more days per year has been increasing and is projected to grow even with dramatic cuts in greenhouse gas emissions. Currently, about 30% of the world's human population is exposed to such deadly conditions each year.

Numerous examples, such as the 2003 European heatwave that killed approximately 70,000 people, the 2010 Moscow heatwave that killed 10,000 people and the 1995 Chicago heatwave that killed 700 people are staggering examples of the risk to life posed by heatwaves. But beyond these highly cited examples, little was known about how common such killer heatwaves are.

The international group of researchers and students coordinated by the University of Hawaii at Manoa set out to answer that question. From over 30,000 relevant publications, the researchers identified 911 papers with data on 1,949 case studies of cities or regions, where human deaths were associated with high temperatures. From those cases, dates were obtained for 783 lethal heatwaves in 164 cities across 36 countries, with most cases recorded in developed countries at mid-latitudes. Some of the cities that have experienced lethal heatwaves included New York, Washington, Los Angeles, Chicago, Toronto, London, Beijing, Tokyo, Sydney and Sao Paulo.

When analyzing the climatic conditions for those cities, the researchers discovered a common threshold beyond which temperatures and humidities became lethal. In agreement with human thermal physiology, the threshold was such that as relative humidity increases, lower temperatures become lethal.

"Finding a threshold beyond which climatic conditions turn deadly is scientifically important yet frightening," said Farrah Powell, a UH Manoa graduate student and one of the co-authors in the study. "This threshold now allows us to identify conditions that are harmful to people. And because it is based on documented cases of real people across the globe, it makes it that more credible and relevant. The scary thing is how common those deadly conditions are already."

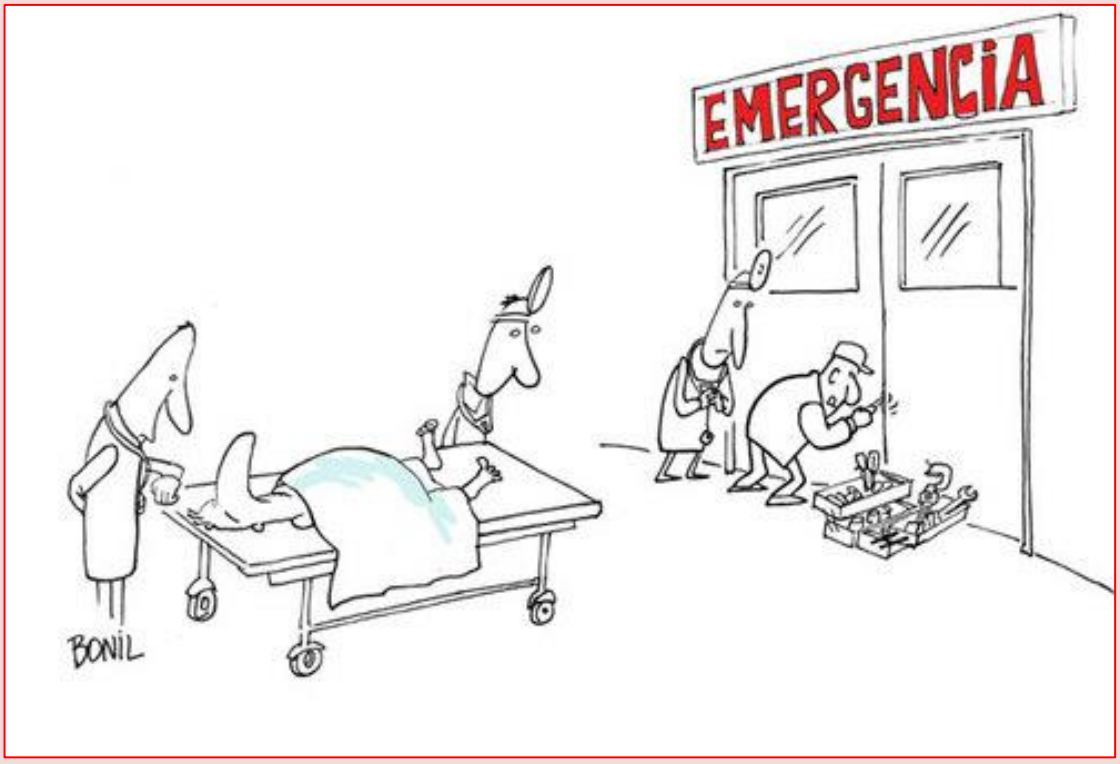
A web-application accompanying the paper allows counting, for any place on Earth, the number of days in a year when temperature and humidity exceed such a deadly threshold. For example, by 2100 New York is projected to have around fifty days with temperatures and humidities exceeding the threshold in which people have previously died. That same year, the number of deadly days for Sydney will be 20, 30 for Los Angeles, and the entire summer for Orlando and Houston.

The study also found that the greatest risk to human life from deadly heat was projected for tropical areas. This is because the tropics are hot and humid year round, whereas for higher latitudes the risk of deadly heat is restricted to summer.

"Warming at the poles has been one of the iconic climatic changes associated with the ongoing emissions of greenhouse gases," said co-author Iain Caldwell, a UH Manoa post-doctoral researcher. "Our study shows, however, that it is warming in the tropics that will pose the greatest risk to people from deadly heat events. With high temperatures and humidities, it takes very little warming for conditions to turn deadly in the tropics."

"Climate change has put humanity on a path that will become increasingly dangerous and difficult to reverse if greenhouse gas emissions are not taken much more seriously," says Mora. "Actions like the withdrawal from the Paris agreement is a step in the wrong direction that will inevitably delay fixing a problem for which there is simply no time to waste."

— Read more in Camilo Mora et al., "Global risk of deadly heat," Nature Climate Change (19 June 2017).



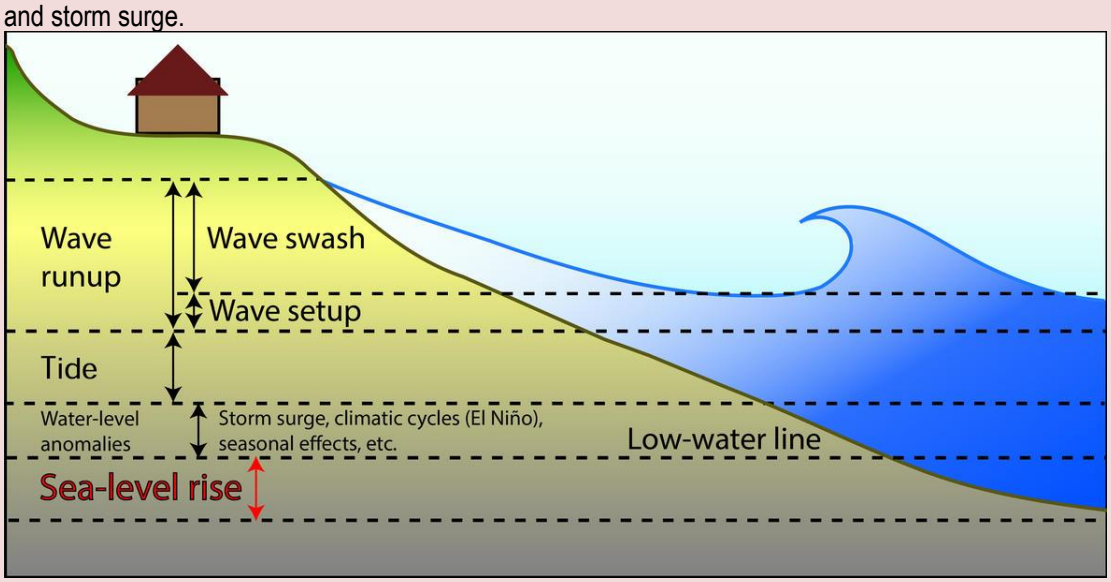

IOI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
ASYMMETRIC
THREATS

Frequency of coastal flooding will double globally in next decades

Source: http://www.homelandsecuritynewswire.com/dr20170531-frequency-of-coastal-flooding-will-double-globally-in-next-decades

May 31 – **The frequency and severity of coastal flooding throughout the world will increase rapidly and eventually double in frequency over the coming decades even with only moderate amounts of sea level rise**, according to a new study published today in *Scientific Reports*. This increase in flooding will be greatest and most damaging in tropical regions, impairing the economies of coastal cities and the habitability of low-lying Pacific island nations. Many of the world's largest populated low-lying deltas (such as the Ganges, Indus, Yangtze, Mekong and Irrawaddy Rivers), also fall in or near this affected tropical region.

USGS says that the new report from scientists at the U.S. Geological Survey, the University of Illinois at Chicago and the University of Hawaii shows that with just 10 to 20 cm (4 to 8 inches) of sea level rise expected no later than 2050, coastal flooding will more than double. This dramatic increase in coastal flooding results from rising sea levels combined with storm-driven flooding, including the effects of waves and storm surge.



In most coastal regions, the amount of sea level rise occurring over years to decades is small, yet even gradual sea level rise can rapidly increase the frequency and severity of coastal flooding. Until now, global-scale estimates of increased coastal flooding due to sea level rise have not considered elevated water levels due to waves, and thus have underestimated the potential impact.

The researchers combined sea level projections with wave, tide and storm surge models to estimate increases in coastal flooding around the globe. They found that regions with smaller variations in ocean water levels due to tides, waves and storm surge, common in the tropics, will experience the largest increases in flooding frequency.

"Although it is commonly understood that sea level rise will increase the frequency of coastal flooding, most of that previous scientific work has focused on analyzing tide gauges which capture extreme tides and storm surge, but not wave-driven water levels. Tide gauge data exist only for a limited number of locations around the world. Using models rather than individual tide gauges provides a comprehensive picture of the widespread vulnerability rather than at sparse points where observed data exist," said lead author of the study, Sean Vitousek, who was a post-doctoral fellow at the USGS when he began this study. Vitousek is now a professor in the Department of Civil & Materials Engineering at the University of Illinois at Chicago.

"The key findings are that areas with limited water-level variability, due to small tidal ranges (for example, the Tropics), and more limited ranges in storm water levels (such as the North American West Coast), will experience the largest increases in flooding frequency. In the Tropics, today's 50-year water level event will occur every 5 years with just 10 cm of sea level rise," said USGS geologist and coauthor, Patrick Barnard.

Most previous research has started with expected scenarios of sea level rise and attempted to find the flooding frequency increase. In this new study, the scientists took the opposite approach, finding the amount of sea level rise needed to double the frequency of flooding, while accounting for the uncertainty and year-to-year variability of storm patterns. One of the surprising findings was that it does not take much sea level rise to double the frequency of flooding (particularly in the Tropics). Using this analysis, Vitousek and his coauthors demonstrate that 10 cm or less of sea level rise expected within the next few decades, can more than double the frequency of coastal flooding for many locations across the globe. The areas with smaller increases in flood frequency include areas with very large tidal ranges and those along typical tropical storm paths.

"Most of the world's tropical atoll islands are on average only 1-2 meters above present sea level, and even in the high tropical islands such as Hawaii, Guam, American Samoa, U.S. Virgin Islands, Indonesia, and others, the majority of the population and critical infrastructure is located on a narrow coastal fringe at low elevations (1-2 m above present sea level) and thus susceptible to this increased flood frequency," said USGS geologist and coauthor, Curt Storlazzi.

"These important findings will inform our climate adaptation efforts at all levels of government in Hawaii and other U.S. affiliated Pacific islands," said coauthor Chip Fletcher, Associate Dean and Professor at the School of Ocean and Earth Science and Technology at the University of Hawaii.

— Read more in Sean Vitousek et al., "Doubling of coastal flooding frequency within decades due to sea-level rise," Science Reports 7, Article number: 1399 (18 May 2017).

Tweet

Heat island effect could double climate change costs for world's cities

Source: http://crisis-response.com/news/news.php?article=1425

June 06 – Overheated cities face climate change costs at least twice as big as the rest of the world because of the 'urban heat island' effect, new research shows.

The study by an international team of economists of all the world's major cities is the first to quantify the potentially devastating combined impact of global and local climate change on urban economies.

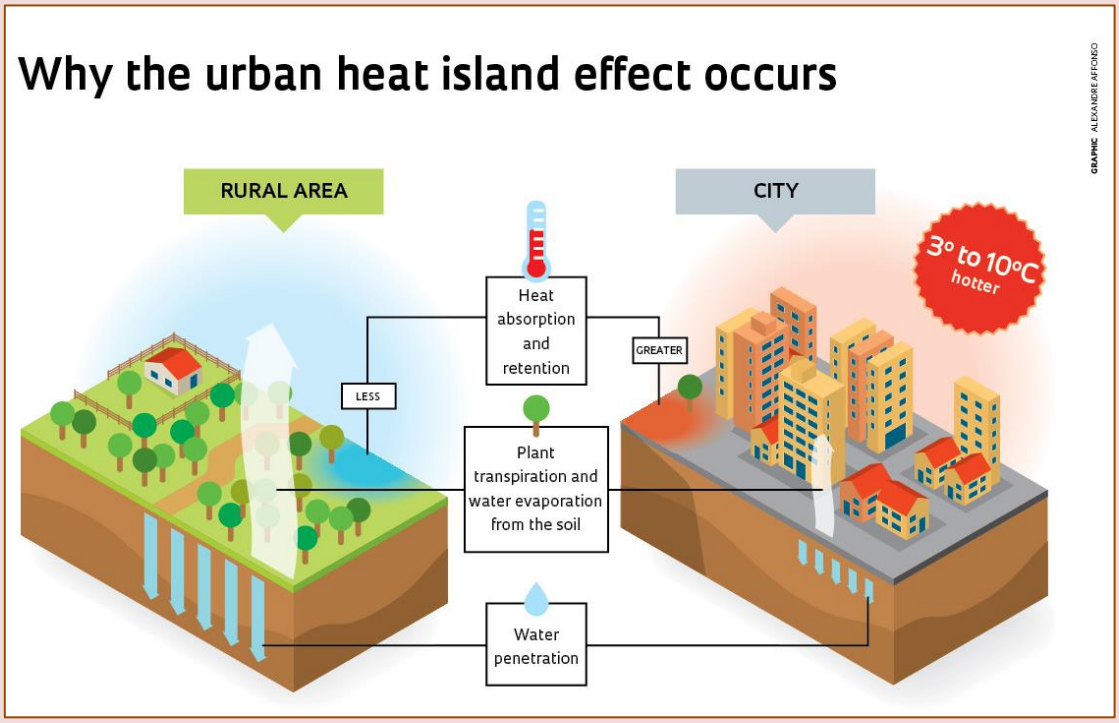
The analysis of 1,692 cities, published at the end of May in *Nature Climate Change*, shows that the total economic costs of climate change for cities this century could be 2.6 times higher when heat island effects are taken into account than when they are not.

For the worst-off city, losses could reach 10.9 per cent of GDP by the end of the century, compared with a global average of 5.6 per cent.

The urban heat island occurs when natural surfaces, such as vegetation and water, are replaced by heat-trapping concrete and asphalt, and is exacerbated by heat from cars, air

conditioners and so on. This effect is expected to add a further two degrees to global warming estimates for the most populated cities by 2050.

The urban heat island occurs when natural surfaces, such as vegetation and water, are replaced by heat-trapping concrete and asphalt, and is exacerbated by heat from cars, air conditioners (photo: Mindaugas Gelunas/123rf)

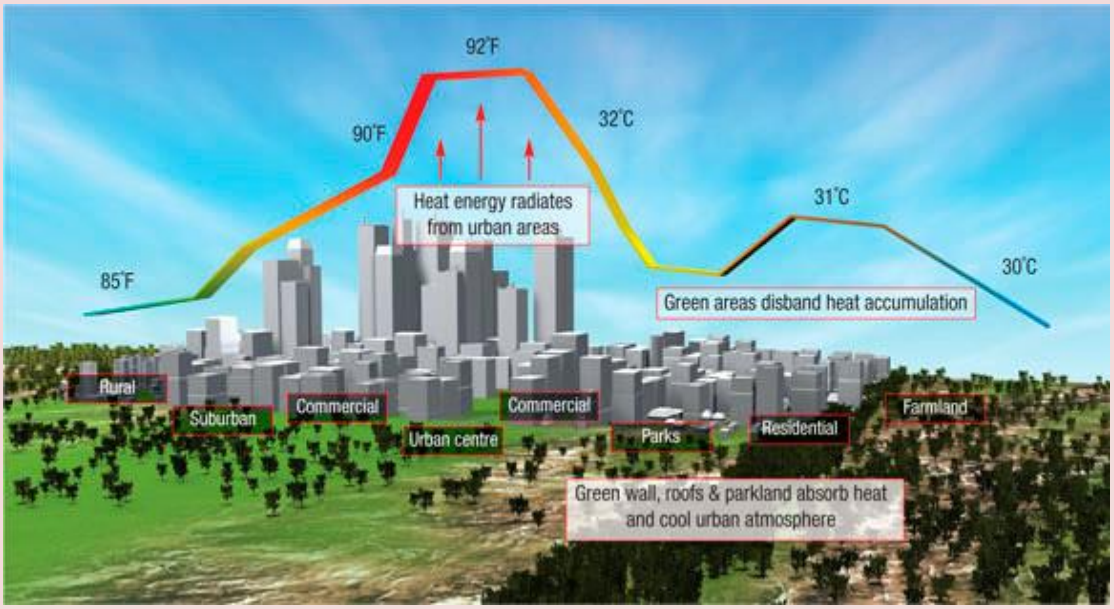


Higher temperatures damage the economy in a number of ways - more energy is used for cooling, air is more polluted, water quality decreases and workers are less productive, to name a few.

The authors – from the University of Sussex in the UK, Universidad Nacional Autónoma de México and Vrije University Amsterdam – say their new research is significant because so much emphasis is placed on tackling global climate change, while they show that local interventions are as, if not more, important.

Professor Richard S J Tol MAE, Professor of Economics at the University of Sussex, said: "Any hard-won victories over climate change on a global scale could be wiped out by the effects of uncontrolled urban heat islands.

"We show that city-level adaptation strategies to limit local warming have important economic net benefits for almost all cities around the world."



Although cities cover only around one per cent of the Earth's surface, they produce about 80 per cent of Gross World Product, consume about 78 per cent of the world's energy and are home to over half of the world's population. Measures that could limit the high economic and health costs of rising urban temperatures are therefore a major priority for policymakers.

The research team carried out a cost-benefit analysis of different local policies for combating the urban heat island, such as cool pavements – designed to reflect more sunlight and absorb less heat –cool and green roofs and expanding vegetation in cities.

The cheapest measure, according to this modelling, is a moderate-scale installation of cool pavements and roofs. Changing 20 per cent of a city's roofs and half of its pavements to 'cool' forms could save up to 12 times what they cost to install and maintain, and reduce air temperatures by about 0.8 degrees.

Doing this on a larger scale would produce even bigger benefits, but the vastly increased costs mean that the cost-benefit ratio is smaller.

The research has important implications for future climate policy decisions – the positive impacts of such local interventions are amplified when global efforts are also having an effect, the study shows. Professor Tol said: "It is clear that we have until now underestimated the dramatic impact that local policies could make in reducing urban warming.

"However, this doesn't have to be an either/or scenario. In fact, the largest benefits for reducing the impacts of climate change are attained when both global and local measures are implemented together.

"And even when global efforts fail, we show that local policies can still have a positive impact, making them at least a useful insurance for bad climate outcomes on the international stage."

Emerging Risk Report – CBRN

The threat of asymmetric attack methods

June 2016

Source: https://www.poolre.co.uk/Reports/Emerging-Risk-Report.pdf

The difficulty of predicting the future is no warrant to ignore it.
Brian Hayes, American Mathematician

The cost of 9/11 demonstrates the scale of damage that can be inflicted by asymmetric attack methods. No one predicted the nature of the attack, or even the intent of Islamic militant groups to fly tonnes of aviation fuel into the heart of the US financial and military establishment. Such attacks, involving mass causalities and unconventional methods of delivery, are clearly rare and catastrophic events due to the difficulties in planning and execution, as well as significant improvements in law enforcement and intelligence practices. However, today's threat actors undoubtedly aspire to emulate these types of mass-causality events.

Costs of 9/11 to the US

	USD billions
4 civilian aircraft destroyed	0.4 bn
World Trade Centre (replacement costs)	3—4.5 bn
Damage to the Pentagon, up to	1 bn
Clean-up costs	1.3 bn
Property and infrastructure damage	10—13 bn
Federal emergency funds	40 bn
Heightened airport security, sky marshals, government takeover of airport security, new in-aircraft security measures, cost of operations in Afghanistan	
Direct job losses: 83,000. Lost wages	17 bn
Level of damaged or unrecoverable property	21.8 bn
Losses to NYC	95 bn
Lost jobs, taxes, damage to infrastructure, cleaning	
Losses to the insurance industry	40 bn
Loss of air traffic revenue	10 bn
Fall of global markets	incalculable

Source: Institute for the Analysis of Global Security

The challenge now is to try and predict the next catastrophic terrorist event and not merely react to it. Although a high degree of accuracy is hard to achieve with events shaped by human behaviour, there is a significant body of intelligence which suggests that the next catastrophic terrorist event could quite possibly involve a chemical, biological, radiological or even nuclear ('CBRN') component. The evidence for this is clear, present and dangerous: the continued use of chemical IEDs in Syria, Iraq and Jakarta; Daesh websites and social media chatter declaring their intent to develop a radiological capability; the FBI Moldovan sting operation that prevented the sale of radiological material to Islamic militant groups; and the recent unconfirmed reports of a Daesh-affiliated anthrax plot in Kenya (May 2016). The perpetrators of the Brussels attacks were also reported to have been conducting surveillance on a senior official in Belgium's nuclear research and development programme.

As pressure on Daesh intensifies, the possibility of more fighters returning back to their home countries increases the threat of a transfer of technology, operational tactics and weapons used in the Middle East to a wider global setting. Asymmetric uses of CBRN devices provide shock, awe and mass casualties, a lure that Daesh would be unlikely to ignore as their territorial hold in Iraq and Syria shrinks.

It should be stressed that conventional CBRN weapon systems represent a highly advanced capability, with significant barriers to acquisition, production, weaponisation and delivery. Current intelligence assessments conclude that Daesh's aspirations exceed their capability to unleash a chemical or radiological device against a Western target, but they are investing significant resources into enhancing this capability. In spite of the many technological barriers, it is usually the psychological impact of these weapon systems that has the potential to cause widespread panic and significant economic losses, irrespective of the success of an attack.

The concern is not that terrorist groups are on the brink of acquiring a fully-operational CBRN capability — the technical barriers, particularly in the case of nuclear and biological weapons, entail that these weapon systems generally only reach their destructive potential at the hands

of nation states. Rather, there is a justified concern about the psychological and economic impacts of chemical and radiological weapons deployed in an unconventional setting. What would the effects of a partially successful chemical or radiological device be? The kinetic effects may be limited — the device may not fully function, the chemical or radiological payload may be consumed in the explosion — but how would the public react and what would the levels of interruption to business be? These are important questions for the (re)insurance industry. As the principal terrorism reinsurer of commercial property in the UK there is a need for Pool Re to monitor the threat landscape to identify changes and developments in terrorists' tactics and capability.

Pool Re and CBRN

Since 2003, Pool Re has provided cover for acts of terrorism involving CBRN attack methods to their full insured value. In recognition of changing threat landscape, and increase in threat actors with the intent to deploy CBRN-enabled devices, Pool Re is currently working with Cranfield University, in association with Guy Carpenter, to enhance our understanding of the possible effects of such attacks on the UK. The research will ultimately produce a detailed loss estimation model for CBRN attacks that could affect Pool Re's exposure across the UK. The model, designed to deal with a number of CBRN attacks and scenarios, is set to be the first of its kind to quantify this peril to the level of detail required. It will involve the use of sophisticated computational fluid dynamics to accurately assess how such agents would behave in an urban environment, such as London. It is assessed that the model will provide a valuable risk mitigation tool and have research applications beyond the (re)insurance market.

Ed Butler CBE DSO
Head of Risk Analysis, Pool Re.

NCT CBRNe USA Paper: The Development of Asymmetric RN Threats Worldwide

By Guillermo Velarde, José Manuel Perlado and Natividad Carpintero-Santamaría
Institute of Nuclear Fusion (IFN), Polytechnic University of Madrid, Spain (2016)
Source: http://www.cbrneportal.com/wp-content/uploads/2016/05/The-Development-of-Asymmetric-RN-Threats-Worldwide.pdf

ABSTRACT

In 2008 the European Union Council adopted the New Lines for Action in Combating the Proliferation of Weapons of Mass Destruction and their Delivery Systems. Main objectives of this strategy are to take measures to combat intangible transfers of know-how, and to intensify efforts to combat proliferation financing, among others. The policy of some countries that want to develop nuclear weapons is worrisome, as they begin to sign the Non Proliferation Treaty (NPT).

But the full scope of nuclear threat encompasses not merely nuclear proliferation. The transnational nature of nuclear and radiological terrorism threat is a matter of great concern. Although the acquisition of weapon-grade uranium is a challenging task for a terrorist organization and the probability that a terrorist group could make an improvised nuclear device or crude nuclear bomb is very small, a real threat includes that a terrorist group, either acting independently or acting as part of a bigger organization, could explode a radiological dispersion device or dirty bomb. According to the 2014 Annual Report of CNS Global Incidents and Trafficking Database, in the last two years 325 incidents of illicit trafficking of radioactive materials have occurred in 38 different countries.

Preventing illicit trafficking in radioactive materials is of paramount importance due to the possibility that they could be transported by people who might enter clandestinely into Western countries. As reported by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex), during the first, second and third quarter of 2015, 2,585 clandestine entries were detected at EU border crossing points.

Nuclear proliferation and radiological terrorism are unequivocally threats worldwide. Reinforcing the multilateral non-proliferation regime and combating the asymmetric threat posed by radiological terrorism are main issues where international collaboration plays a key role in the globalized context of international security.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
BUSINESS
CONTINUITY
OPEN FOR
BUSINESS
AS USUAL
Business Interruption
Disaster Event

Latest Strategic guidance on Building decontamination for CBRN

Source:http://www.continuityforum.org/sites/default/files/images/403486_HMGov_StrategicNationalGuidance_acc.pdf

The guidance is part of sensible contingency and business continuity planning and does not mean that there is an increased risk of terrorist attack using CBRN materials. It gives basic information on the decontamination and remediation that may be required following a deliberate or accidental release in the UK as outlined below.

This document replaces guidance published in 2004 by the Department for Environment, Food and Rural Affairs, and the Office of the Deputy Prime Minister (now the Department for Communities and Local Government).

An incident, whether deliberate or accidental (HazMat), involving chemical, biological, radiological or nuclear materials can potentially lead to the loss of life, contamination of the built and open environment, disruption of society and consequential damage to the UK economy. It is therefore important that plans are in place to minimise the effects of such an event, and to plan for recovery following this type of incident.

This guidance builds on the 2004 documents, and offers improved signposting and updated information in a shorter and more accessible format. It also covers key elements in the decontamination process following an incident – from developing the initial recovery strategy through to managing waste and returning things to normal.

The principal roles and responsibilities of key organisations have been identified and listed, and planning and precautionary measures have been highlighted to promote better preparedness.

In view of the different types of potential incidents, and the variety of buildings, environments and infrastructure that could be affected, the guidance in this document is necessarily generic. It provides a starting point for the development of more detailed contingency plans to deal with specific incidents. This document also describes the current legal powers available to local authorities in the event of such an incident.

Be Prepared: CBRN Substances and Terrorism

By Roger C. Stokes

Source: https://www.crawfordgts.com/media-center/techtalk/2010-v1-1/be-prepared-cbrn-substances-and-terrorism.aspx

Is the developed world adequately prepared for the threat of a terrorist attack using chemical, biological or radiological/nuclear (CBRN) weapons?

Certainly, awareness of and communication about terrorist activity has improved in the wake of the Sept. 11, 2001, attacks in the United States. The U.K. government has increased its threat level and introduced various counter-terrorism measures. As of January 2010, the current threat level there was assessed as "severe," which is the second highest threat level and is defined as "an attack is highly likely." At this writing, the U.S. government's national threat level is "elevated" (yellow), which means there is a "significant risk of terrorist attacks."

However, the nature of the terrorist threat has evolved over recent years and can take a number of forms, including explosive devices, firearms and missiles. As well as "traditional" terrorist acts, which focus on immediate death and destruction, there is a growing risk that attacks will become more diverse and sophisticated and CBRN devices may become part of the terrorist arsenal.

To date, no such incidents have taken place in the U.K., but cases in the United States, such as the deadly anthrax attacks of 2001, highlight the scale of damage such a terrorist act could cause. Damages due to the anthrax attack exceeded $1 billion, according to FBI reports.

Radiological attacks could potentially cause even more severe problems. The much-hyped "dirty bomb" may not be the greatest risk to life when its immediate effect is compared to that of conventional explosives, but just one such device could render large areas of property uninhabitable for a considerable period of time. Removal of radioactive material is very different from removing toxic smoke contamination following a fire or explosion.

Over the last five years, much work has been carried out by world governments, technical experts, manufacturers and specialist contractors in monitoring and preparing to respond to

terrorist threats involving CBRN substances. Research programs are continuing and some progress has been made in the use of specialist tools and techniques, many of which were not available a few years ago. It is important that adjusters are aware of the issues surrounding CBRN terrorism, the various bodies that would become involved in response and recovery activities, and protocols and recommendations for an effective insurance industry reaction to such incidents.
Note: while the general concepts in this article are universal, many specifics concerning preparedness, response and recovery focus on the United Kingdom.

CBRN Weapons and Dirty Bombs
The chart below outlines types of CBRN substances and weapons and the impact and recovery efforts that can be expected if they are deployed.

CBRN Weapons

Substance	Form	Deployment*	How it enters the body	Decontamination	Other information
Chemical	Liquid or gas	Spray Volatile liquid Gas In food and water	Contact, inhalation, ingestion	Successful decontamination techniques and experience exists.	Highly volatile compounds quickly disperse in open air, which can result in minimal dosages to intended victims. Generally more lethal when used in closed spaces Low-volatility materials can linger. Have been used in conflicts such as Iraq and World War I.
Biological	Wet or dry powder containing bacteria, viruses, toxins or fungi from living organisms	Spray Person-to-person In food and water	Contact, inhalation, ingestion	Some successful decontamination techniques have been developed. Vaporized hydrogen peroxide/chlorine dioxide has been successfully used in trials and real bio-terrorism incidents.	Developed for biological warfare Relatively easy and inexpensive to obtain. Many can be grown in fermenters such as those used by pharmaceutical companies. Create panic through fear of the unknown Deployment can be difficult Can overwhelm medical services Diagnosis and treatment can be difficult. Symptoms can take days or weeks to appear, although recent developments have been made in rapid detection capability for some substances, such as Ricin.
Radiological	Radioisotopes (substances that produce alpha, beta or gamma radiation). Amount of radioactivity emitted by those substances varies significantly.	Dirty bomb or radioactive dispersion device (RDD) Spray Fire In food and water	Contact, inhalation, ingestion	Highly specialized techniques are available for removal of radioactive material. Very different from removing toxic smoke	A dirty bomb disperses radioactive material in a wide area using a conventional explosive. The radioactive material plays no part in detonating the bomb. Large areas can be made uninhabitable for a considerable period of time.

				contamination following a fire or explosion. Most effective decontamination technique is usually physical removal of material, but that depends on the type of surface that is contaminated.	
Nuclear	Nuclear reaction (fission or fusion) that releases vast quantities of energy and damages through blast, fire and release of harmful radiation	Explosive nuclear device including trigger (neutron generator)	Contact (also inhalation, ingestion for survivors of initial blast)	The blast site and large areas surrounding it must be abandoned due to radioactive fallout. Long-term decontamination program as described for radiological substances is necessary.	A 10-kiloton nuclear explosion (small tactical nuclear weapon or sophisticated terrorist design) would lead to a circle of near-total destruction approx. 2 miles in diameter. Not believed to be a significant risk from any terrorist group at present.

* Influenced by weather conditions including precipitation, wind strength/direction and humidity.

Though all weapons pose threats, the dirty bomb may be the one most on people's minds today. A quick scan of the media will uncover many stories warning of the increasing threat posed by dirty bombs. According to a London Daily Mail article published March 23 of this year, a recently developed counter-terrorism strategy for the U.K. finds that the threat of a dirty bomb is rising because "there has been a significant increase in the trafficking of material that can be used in radiological and conceivably nuclear weapons."

The International Atomic Energy Agency (IAEA) in Vienna attempts to keep track of many kinds of radioactive materials as they move around the globe. However, security standards reflect the degree of hazard presented by each material. Since the types of radioactive materials that can make up dirty bombs are used extensively in medicine, industry, agriculture and research, they can be easier to acquire than materials that would be required to produce a nuclear explosion.

The greatest impact of a dirty bomb might be psychological rather than physical. It is likely that any immediate fatalities would result from the explosion itself rather than any impact from the nuclear material. While anyone coming into contact with radiation increases his or her risk of developing cancer, following the detonation of a dirty bomb, only those who receive extremely large doses and are unable to be decontaminated quickly could potentially suffer radiation sickness.

However, because significant exposure can be fatal, and because we cannot taste, smell, feel or see radiation, dirty bombs may be especially frightening to people. In testimony before the U.S. Congress, Richard Meserve, former chairman of the U.S. Nuclear Regulatory

Commission, said the health consequences from the use of a dirty bomb would be minimal and the greater concern is a "psycho-social one." He added, "The terrorist's greatest weapon is fear."
While the overall impact of dirty bombs on health and life might be unclear, there is no doubt that cleaning up after a dirty bomb would likely be time-consuming and costly, as several incidents involving radiation exposure demonstrate.
In September 1987, a scrap metal merchant in Goiânia, Brazil, opened a lead canister that was taken from an abandoned cancer treatment center. Inside he found a glowing blue powder that turned out to be radioactive caesium chloride. Curious residents living nearby passed the canister from home to home for nearly a week. More than 200 people were exposed to the radiation; four died. Decontamination, which included demolition of 85 homes, reportedly took about three months. Cleanup efforts produced some 3,500 m3 of radioactive waste that was stored in more than 6,000 containers. Two huge repositories were built to house the containers.
It could be argued that in terms of fatalities, the Goiânia event was worse than any potential dirty bomb incident, since there was no explosion and the individuals were initially unaware that they were severely contaminated with radioactive caesium.
The poisoning of former Soviet KGB agent Alexander Litvinenko with the alpha-emitter polonium-210 in November 2006 further demonstrates the problems that can be caused by radioactive contamination of people and properties. Some 50 locations around London were deemed to be contaminated and cleanup was a significant learning exercise for the authorities and government agencies involved. At the height of the operation, the Health Protection Agency deployed some 70 people to oversee all the contaminated sites, with private contractors also working on decontamination. The worst area was in the Millennium Hotel, suspected to be the place where Litvinenko was poisoned; 19 days of cleanup were necessary there.
Preparation, Response and Recovery: Who's Responsible?

Emergency preparedness
In the United States, responsibility for emergency and terrorism preparedness lies with the Department of Homeland Security, which was established in 2003. A U.S. initiative called BioShield was set up with a $5.6 billion budget in 2005 to fund the stockpiling of vaccines and medications for biodefense and develop necessary medical countermeasures against chemical, biological, radiological and nuclear attacks.
Similarly, in the U.K., the Home Office holds primary responsibility for counter-terrorism. In July 2001, it set up the Civil Contingencies Secretariat to improve the "resilience" of central government and the U.K. "Resilience" is defined as the ability to handle any disruptive challenges including terrorism. Various funding has been provided for local authorities, fire services and the NHS.
In 2004, the U.K. government issued the Civil Contingencies Act, which includes local arrangements for civil protection and establishes a statutory framework of roles and responsibilities for local responders, legislation and use of special legislative measures. Although the Act refers to chemical, biological and radiological incidents, it contains no detail about specific measures to deal with them.
Emergency response and recovery
In a CBRN emergency, U.K. police would lead a response phase as Gold Command, the most strategic level of the command structure used by U.K. emergency services, and would chair a Strategic Co-ordinating Group (SCG).
A recovery effort would be led by the organization with the most appropriate combination of responsibility, capability and management capacity - most likely, a local authority that can draw together all appropriate parties into a multi-agency effort.
The SCG would most likely task a Recovery Working Group (RWG) to bring key agencies together to give momentum to the recovery management effort within an overall strategic framework. It would form the focus for integrated initiation of and planning for recovery, while ensuring the coherence of response and recovery work. It would be led by a senior officer of the agency most appropriate to the task. In many cases, this will be the local authority, given its functions in relation to the remediation of the physical environment, coordination of welfare support and community leadership.
The RWG would seek to:

- Ensure that longer-term recovery priorities are reflected in the planning and execution of the response.

- Ensure that relevant organizations in the public, private and voluntary sectors are engaged in the recovery effort from the earliest opportunity.
- Ensure continuity of emergency management once the response phase concludes.

Decontamination

It is likely that any longer-term cleanup operation would be beyond the capabilities of existing damage mitigation companies. Emergency services are likely to concentrate on mass decontamination of people and mitigating the spread of CBRN material.

To address long-term cleanup issues, the U.K. Department for Environment, Food, and Rural Affairs (DEFRA) established the Government Decontamination Service (GDS) in 2005. This organization, which has linked with many similar government departments throughout the world, is designed to increase the U.K.'s capacity to resist and recover from deliberate and accidental releases of CBRN materials and hazardous substances. The primary objectives of the GDS are:

- To establish and maintain a framework of contractors that can offer appropriate remediation or decontamination-related services.
- To test, exercise and evaluate GDS and GDS framework capability
- To capture information on known framework capability and capacity, identify gaps in known capability and capacity, and explore mitigations and possible solutions as appropriate.
- To participate in identifying, prioritizing and, as necessary, managing decontamination-related research projects.
- To build up a library of relevant knowledge and experience on remediation.
- To maintain a duty officer to give access to GDS services at all times.

Crawford & Company has discussed CBRN recovery techniques with a number of companies, many of which have experience cleaning up chemical, biological and radiological contamination, although clearly none have been tested in a response to a real CBRN terrorist incident. However, Crawford has shared some of its expertise with DEFRA and continues to discuss the important links between the GDS and the insurance industry.

The Role of the Insurance Industry in CBRN Incidents

The insurance industry is highly likely to be a key stakeholder following any CBRN terrorist incident and will need to play a significant part in the clearance, decontamination and recovery phases. Loss adjusters and their specialists require information at an early stage and access to the scene for their needs to be considered.

In the U.K., a joint protocol has been developed to ensure that this need is recognised and enable cooperation between the various responding services and agencies. Parties to this protocol, called "The Role of the Insurance Industry in Dealing with Civil Emergencies," include:

- ABI - Association of British Insurers
- CILA - Chartered Institute of Loss Adjusters
- Air Accidents Investigation Branch
- Local Government Association
- Chief Fire Officers' Association
- Association of Chief Police Officers.

The protocol provides for a principal point of contact within a Gold Command/SCG to liaise with a principal point of contact acting on behalf of the insurance industry. The insurance industry contact will be provided with details of the event at the earliest opportunity. Representatives(s) of the insurance industry will be allowed access, as and when

appropriate, to carry out necessary insurance investigations. Similarly, representatives of the insurance industry also will be invited to join any RWG that may be established.

In the recovery phase, the private sector will play a significant part, given the size of the resources, specialist expertise and capabilities (e.g. site clearance, decontamination and engineering) at its disposal. Private sector companies also have a direct commercial interest in ensuring the remediation of sites and the rapid rehabilitation of the communities they operate in.

Other issues insurers and adjusters should keep in mind in the event of a CBRN attack are:

- In the event of a terrorist attack involving CBRN substances, access to any affected site for representatives of the insurance industry will be restricted until clean-up measures are implemented by, in all probability, one of the GDS contractors or other specialist firms. Site visits by adjusters could be delayed for months, or even years, until an area is decontaminated. Adjusting activities will therefore concentrate on remote implementation of business continuity plans and business recovery, and probably re-housing at alternative locations. It is likely that any alternative location will need to be at a considerable distance from the terrorist site.
- Emergency services will concentrate on the mass decontamination of people and mitigating the spread of CBRN material. It is important that the right specialists are used at the initial stages to help with decisions on mitigation. Proper liaison via nominated insurance industry contact to the Gold Command/SCG/RWG will be essential to ensure that the needs of our industry our met. This includes mitigation, decisions on decontamination, cost control, project management and business interruption aspects.
- It is likely that initial damage and contamination appraisals will be carried out by specialists, working on behalf of loss adjusters, who are familiar with the substances involved and adequately trained in the use of CBRN personal protective equipment (PPE). They would be our eyes and ears, perhaps using a combination of video recording and photography in association with their contamination assessments.
- Any longer-term clean-up operation would probably be beyond the capabilities of existing damage mitigation companies. Crawford has contacts with companies that are able to decontaminate buildings and property involving CBRN material. However, availability of equipment and qualified personnel to carry out long-term decontamination operations is severely limited. Nevertheless, we understand that the GDS is identifying personnel and equipment on a global basis and this information will be invaluable in our response to decontamination issues.

Resources

For more information on the various organizations and initiatives mentioned in this article, go to:

- U.K. Home Office (counter-terrorism)
  http://www.homeoffice.gov.uk/counter-terrorism/
- U.K. Resilience
  http://www.cabinetoffice.gov.uk/ukresilience.aspx
- U.K. Government Decontamination Service
  http://www.defra.gov.uk/gds/
- U.S. Department of Homeland Security
  http://www.dhs.gov/index.shtm
- U.S. Department of Health and Human Services (BioShield)
  http://www.hhs.gov/
- International Atomic Energy Agency
  http://www.iaea.org/

Roger Stokes *joined Crawford in 1992 after working in process design, operations and troubleshooting, production and management in the chemical industry for more than 10 years. A chemical engineer by training and chartered engineer in the U.K., he is based in the Power & Energy Division of Global Technical Services and has handled major chemical, petrochemical and refinery losses world-wide.*

Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy for Canada

Source: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-strtg/index-en.aspx

The threat of chemical, biological, radiological, nuclear and explosives (CBRNE) events is a global challenge. Terrorist attacks are increasingly focused on western interests and Canada has been specifically identified as a target by terrorist organizations. Canada is also at risk from domestic sources such as radicalized individuals, extremists and criminals. This threat, aggravated by the prevalence of potential CBRNE materials normally used for industrial and scientific purposes, requires coordinated action by many contributors.

In order to enhance and sustain Canada's resilience to CBRNE events, all levels of government within Canada have collaborated to develop the *Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy for Canada* (hereafter referred to as "The Strategy"). Its purpose is to provide the policy framework that will guide the creation of sustainable capabilities and common standards in CBRNE policies, programs, equipment and training.

The Strategy promotes the vision of an integrated capability across Canada by framing a scalable, responsive, dynamic, sustainable and evidence-based approach for all contributors to CBRNE events. This approach is equally based on the Four Components of Emergency Management: prevention / mitigation, preparedness, response and recovery.

The Strategy is based upon five key strategic objectives that have been agreed upon as fundamental if Canada is to achieve sustainable resilience to the risks and threats of CBRNE events. They are:

1. **Leadership -** to guide coordinated policy and program development by all levels of government and contributors that will foster and promote CBRNE resilience;
2. **Risk Management -** to integrate CBRNE into a consistent all-hazards risk management approach, including robust hazard, vulnerability and risk assessment methodologies;
3. **Capability-based Planning -** to inform policy, program and investment decisions based on the principles of capability-based planning.
4. **Effective and InteroperableWorkforce -** to build an effective and interoperable workforce that is supported by a modern, dynamic and responsive training infrastructure backed up by appropriate technologies; and
5. **Information and Knowledge Management -** to develop effective information, knowledge and intelligence managements systems and mechanisms across all jurisdictions and contributors.

An Action Plan, which is an integral part of this Strategy, sets out actions and timelines for CBRNE programs and activities over a five-year period. The Action Plan is based on the five strategic objectives. Efforts in support of the Action Plan identify and strengthen the capabilities across Canada to prevent / mitigate, prepare for, respond to, and recover from CBRNE events. All levels of government will work collaboratively to monitor the implementation of the Strategy and Action Plan. Together, these efforts will enhance CBRNE resilience in Canada.

Terrorism: business continuity, behaviour and barriers

Source: http://www.thebci.org/index.php/terrorism-business-continuity-behaviour-and-barriers

In the closing months of 2015, two particular acts of terror in different western countries had an important effect on the international and domestic threat landscape. BC practitioners working within the sphere of organisational resilience should be aware that the

consequences of these events will probably impact on their responsibilities. The following article comments on the prevailing threat background, current ideas on response, notes on situational awareness and concludes with some lessons for all of us with a responsibility for BC.

The changing face of terror

On 13 November 2015, a series of coordinated terrorist attacks occurred in Paris, leaving 130 dead and 368 wounded (similar to the attack in Mumbai in 2008). None of the victims were personally known to the attackers. Seven of the perpetrators also died during the deadliest terrorist assault within the EU since the Madrid train bombings in 2004. France had been on high alert since the January 2015 attacks in Paris that killed 17 people.

On 2 December 2015, a married couple living in California, shot and killed 14 people at an office party in San Bernardino and injured 22 more. Many of the dead were personally known to at least one of the attackers who was a co-worker in the same office. The perpetrators also left three explosive devices connected to one another at the scene in the hope that casualties would be even higher after the initial shooting.

It is particularly worrying that the terrorists behind the Paris attacks combined an element of substantial planning (large public targets, substantial weaponry and a suicidal endgame) with the unpredictability of a marauding assault, meaning that we now have in Europe gun attacks, marauding or focused, as an enduring security challenge, rather than just a random one-off event.

In the case of the San Bernardino shooting, what appeared to be yet another active shooter incident in America (US 2015 – 353 shootings of more than one person, 62 shootings at schools, 12,223 people killed in gun incidents, 24,722 people injured in gun incidents1) turned out to be a terrorist attack that has now changed how such events are categorised in that country.

In the US, almost 100% of active shooters are male, just over half occur in office environments and in roughly 80% of such incidents there is a connection between the shooter and at least one of the victims (family, academic, professional etc.). Syed Farook was known at work to occasionally use anti-Jewish rhetoric and with the benefit of hindsight, exhibited some characteristics of a potential active shooter, noting that his profile on a dating website called iMilap includes 'reading religious books' and 'hanging out in back yard doing target practice'. But it was the involvement of his wife and fellow assassin, Tashfeen Malik, who changed things.

According to a relative in Pakistan "she started taking part in religious activities and also started asking women in the family and the locality to become good Muslims". She was also the first to pull the trigger when the couple shot her husband's work colleagues and reportedly swore allegiance to the leader of so called IS on Facebook, the day before the murders. Moreover, the equipment used by the pair (homemade pipe bombs, military vests and heavy calibre weapons), was similar to IS terrorist attacks elsewhere. As a result, it is now difficult to make reasonable distinctions between an active shooter and a terrorist to help predict and deter such separate types of attack and their impact in the work environment, especially when the threat level in the UK for example, remains high.

Some current ideas on response

At the time of writing this article the official UK terrorist threat level is 'severe', meaning an attack is thought to be 'highly likely'. Scotland Yard say there have been at least six attempts to carry out an attack of some sort in 2015 where arrests for suspected terrorist offences are running at an average of one a day. The UK has been warned.

In which case, what is the current advice in tackling this type of menace and what in particular should a BC practitioner be thinking? I have outlined here the difference between the US and UK, plus an idea from Paris post November 2015 and what at least one of our own BC clients is already doing.

In the UK the advice when confronted by an active shooter is 'Run, Hide, Tell'. Run, if you can, if you can't run, hide and then, when you can, tell the police what's happening so they can get help there quickly. UK Government advice also includes the sentence "if someone is in immediate danger and their life is being threatened we would never criticise their actions if instinct takes over and they feel the need to fight back". A somewhat British understatement in the extreme drama of an active shooter, compared to advice from other countries which, in some cases, have more experience than the UK when it comes to such atrocities.

In the US and some other countries, the advice is 'Run, Hide, Attack'. In short, fight before tell, unlike the UK, although suggestions on stacking chairs/tables as barriers in a hopefully safe room are common to each. The American advice is the result of analysis of 160 active shooter events which showed that in 21 cases unarmed civilians managed to overpower a gunman. However, in most UK offices, there is seldom a pair of scissors or blunt object at hand to use against the assailant, since fighting an armed attacker has to be with considerable/deadly force. Also, most office workers simply would not think this way, but they would use a phone if possible (noting it should be switched to silent to avoid giving a hiding position away). Yet, on the other hand, some heroic people have suddenly done extraordinary things, quite unexpectedly, when faced with a real life or death situation. To tell or to fight is therefore debatable. So what do the French now advise?

In Paris you are now likely to see a poster in many public places (e.g. shopping centres, museums, stadia) which illustrates how to respond to a terrorist attack. Modelled on the 'in the event of emergency' cards for airline passengers, the poster suggests first fleeing, then hiding and then raising the alarm. One picture, on helping fellow victims, even shows a man pulling up a woman who is dangling from a window ledge, recalling an incident that was caught on CCTV in November. Useful to know, but what should an enterprising BC practitioner now be thinking of in terms of actual planning in advance?

One of our UK clients (also with a responsibility for security) has already enacted some logical steps for the various offices that he is responsible for. These include:

- Restrict access to building areas;
- Immediately ground all lifts – without resorting to setting off fire alarms;
- Ensure you are able to quickly communicate with everyone in the building. This includes pre-recorded (or at least prepared) messages;
- Reduce people becoming greater targets for an active shooter in the reception and/or ground floor where an attacker might use a previously seen tactic of breaking the fire alarm glass and thereby triggering an unnecessary evacuation. This means putting ground floor break glass on 'double-knock' where an initial alarm is effectively silent for a brief while, allowing a double check and cancel a false call if confirmed; and
- Organise a rapid assessment and decision making framework where directions can be quickly disseminated.

The last point about assessing, deciding and disseminating has a direct link to one of the key response ingredients to this type of scenario and indeed, all types of crises – situational awareness.

Situational Awareness

BS 11200 (Crisis Management) explains in some detail the essence of situational awareness which is to try and understand:

- What is going on
- What the impacts might be
- The degree of uncertainty
- The level of possible/probable containment
- What exacerbating issues might exist
- What might happen next

However, getting answers to these questions is inherently difficult in crisis scenarios because:

- Many things are probably happening simultaneously
- The situation can change rapidly
- Priorities alter
- Different interpretations of cause and effect might be equally plausible
- Information might not move freely
- Technical knowledge might be required to interpret certain information
- Terminology might not be commonly understood
- Some pieces of information might deliberately be withheld from others for whatever reason
- The possible spread of impacts is almost certainly going to be unclear

It should be noted that for most organisations the ability to create shared situational awareness in a crisis cannot be assumed on the basis of normal operations that function at a routine or 'slow time' tempo (www.bsigroup.com). In any crisis, a 'quick time' decision-making structure should be applied (which is one reason why running at least one scenario exercise in advance is strongly advised).

Lessons for BC practitioners

Responding to these threats requires more than whatever corporate security might exist where you work. The impact and ramifications of scenarios such as Paris and San Bernardino require a much more resilience-focused reaction to anticipate, respond and recover (as shall be discussed at the next World Conference on Disaster Management in Toronto, where the Business Continuity Institute are 'Diamond' sponsors) and this is where any effective BC professional has a key role to play alongside HR, security, risk and other disciplines. The latest BCI Horizon Scan Report featured terrorism as one of the top ten threats that BC professionals worry about for the fourth year running. Here are a few actions to take now:

Understand the threat – If we didn't know before, it's clear that terrorists such as so-called IS have now come to us. They have gone global with attacks that are not random or indiscriminate. In less than a fortnight last year, IS carried out three organised acts of mass murder in as many countries: downing a Russian plane Egypt, a suicide bombing in Beirut and then attacking Paris once more as active shooters. In September 2014, the leading public ideologue of IS called on followers overseas to launch attacks without waiting for permission or specific direction. This call to action – IS styles it a 'fatwa', or religious ruling, so they can convince followers of their divine righteousness – had a profound and immediate effect. It can be directly linked to a series of other attacks so far in Canada, Belgium, Australia and Denmark. On 29 December 2015, a husband and wife team were found guilty of plotting a terror attack in London ahead of the 10th anniversary of the 7 July bombings.

Understand how your people will behave – Many survivors of the Paris attacks said they mistook the first gunshots for fireworks and took no notice. This is very common in many active shooter events as the sound of fireworks is probably the nearest memory reference point for most of us on hearing such noise. Numerous socio/group experiments and real-life situations demonstrate that up to 20% of people exposed to a sudden drama might react in a way that probably helps them survive, but the remaining 80% will remain bewildered, looking to other people to act first. Therefore, your plans (refer to the links in this article) must factor in how people will actually behave, rather than just look impressive on paper.

Understand what you can do now – I have referred above to two separate sources where you can at least download training videos and advice based on run, hide, fight, or run, hide, tell. In addition, I have copied five key ideas from one of our UK-based BC clients.

However, it is the core purpose of BC that should be at the centre of any response to these types of threat. To quote from the BCI GPG "BC helps an organisation to build and improve resilience and provides the capability for an effective response to (any) threatening events". To which I can only add two further comments: First, prepare something now. "All that is necessary for evil to triumph is that good men do nothing." So said one of the UK's greatest parliamentarians, Edmund Burke in the 18th century. Second, convert that action to include at least an exercise in advance, to walk your people through what to do if the worst was to happen. Get them to understand how they and their colleagues ought to react.

So in conclusion, business continuity certainly, behaviour absolutely and barriers maybe.

Reference

(1) Shooting tracker, Gun Violence Archive

Peter Power *BA FIRM JP has been the head of Visor Consultants (UK) Limited since 1995. He is Chairman of the World Conference on Disaster Management, is co-author of BS guide 11200 on Crisis Management and is a past member of the UK National Security Commission (IPPR) under Lord P Ashdown.*

XL Catlin boosts US terrorism insurance limits

Source: http://www.businessinsurance.com/article/20170419/NEWS06/912312979/XL-Catlin-boosts-US-terrorism-insurance-limits

Apr 19 – **XL Group Ltd. (UK), said Wednesday that it has raised its available terrorism insurance coverage limits 25% to $250 million to meet continued demand for terrorism coverage.**

The stand-alone terrorism policy is intended to help U.S. businesses address potential gaps in coverage provided by the federal Terrorism Risk Insurance Program Reauthorization Act, the insurer, which does business as XL Catlin, said in a statement.

XL Catlin's terrorism insurance coverage includes coverage for direct physical loss or damage and resulting business interruption; terrorism liability and general liability for bodily injury and physical damage resulting from an act of terrorism; and a broad definition of terrorism, including coverage for acts perpetrated for political, religious and ideological purposes, according to the statement.

The coverage also includes options to add insurance for chemical, biological, radiological and nuclear, or CBRN, events; active assailant insurance events; and threat of terrorism.

XL Catlin also said it provides its stand-alone terrorism policyholders with access to its retained consultancy, S-RM, a London-based global business intelligence, risk management and cyber security services firm that provides tailored consultancy support for preloss planning and post-loss business continuity services.

"Terrorism events in every corner of the world are prompting businesses worldwide to take a hard look at the risk that terrorism poses to their property and operations," Ben Tucker, head of U.S. terrorism and political violence insurance for XL Catlin, said in the statement. "They are looking for higher levels of financial protection to meet increased terrorism concerns and with this increase, we're better equipped to address more of their coverage needs."

Understanding Terrorism Insurance

Source: http://www.iii.org/article/understanding-terrorism-insurance

Terrorism insurance provides coverage to individuals and businesses for potential losses due to acts of terrorism.

Individuals

Standard homeowners insurance policies include coverage for damage to property and personal possessions resulting from acts of terrorism. Terrorism is not specifically referenced in homeowners policies. However, the policy does cover the homeowner for damage due to explosion, fire and smoke—the likely causes of damage in a terrorist attack.

Condominium or co-op owner policies also provide coverage for damage to personal possessions resulting from acts of terrorism. However, damage to the common areas of a building like the roof, basement, elevator, boiler and walkways would only be covered if the condo/co-op board has purchased terrorism coverage.

Standard renters policies include coverage for damage to personal possessions due to a terrorist attack. Again, coverage for the apartment complex itself must be purchased by the property owner or landlord.

Auto insurance policies will cover a car that is damaged or destroyed in a terrorist attack only if the policyholder has purchased "comprehensive" coverage. Most people who have loans on their cars or lease are required by lenders and leasing companies to carry this optional

form of coverage. People who buy only liability coverage are not covered in the event their vehicle is damaged or destroyed as the result of a terrorist attack.
Life insurance policies do not contain terrorism exclusions; proceeds will be paid to the beneficiary as designated on the policy. Health and disability insurance policies may provide coverage for loss of life, injury or sickness to individuals in the event of a terrorist attack.

Businesses
Prior to 9/11, standard commercial insurance policies included terrorism coverage as part of the package, effectively free of charge. Today, terrorism coverage is generally offered separately at a price that more adequately reflects the current risk.
Insurance losses attributable to terrorist acts under these commercial policies are insured by private insurers and reinsured or "backstopped" by the federal government pursuant to the Terrorism Risk and Insurance Act of 2002 (TRIA). Under TRIA, owners of commercial property, such as office buildings, factories, shopping malls and apartment buildings, must be offered the opportunity to purchase terrorism coverage. TRIA was renewed for a further two years in 2005 and is set to expire at the end of 2007.For the terrorism coverage to be triggered under TRIA for commercial policies, a terrorist attack has to be declared a "certified act" by the Secretary of the Treasury.
No such declaration is needed to trigger coverage under home and auto policies because there are no exclusions for terrorism.

What is not covered?
There are long-standing restrictions regarding war coverage and nuclear, biological, chemical and radiological (NBCR) events in both personal and commercial insurance policies.
War-risk exclusions reflect the realization that damage from acts of war is fundamentally uninsurable. No formal declaration of war by Congress is required for the war risk exclusion to apply. Nuclear, biological, chemical and radiological (NBCR) attacks are another example of catastrophic events that are fundamentally uninsurable due to the nature of the risk. Under the Terrorism Risk Insurance Act, if some NBCR exclusions are permitted by a state, an insurer does not have to make available the excluded coverage.

Business Interruption Insurance
Property damage to commercial buildings from a terrorist attack also may include claims for business interruption. Business interruption insurance (sometimes referred to as business income coverage) covers financial losses that occur when a firm is forced to suspend business operations either due to direct damage to its premises or because civil authorities limit access to an area after the attack and those actions prevent entry to the business

premises. Coverage depends on the individual policy, but typically begins after a waiting period or "time deductible" of two to three days and lasts for a period of two weeks to several months.
Business interruption losses associated with acts of civil authority (e.g., closure of certain area around the disaster) can only be triggered when there is physical loss or damage arising from a covered peril (e.g., explosion, fire, smoke, etc.) within the area affected by the declaration. The loss/damage need not occur to the insured premises specifically. Reductions in business income associated with fear of traveling to a location, in addition to closure to areas by authorities because of a heightened state of alert, would not be covered by business interruption policies.

Workers compensation

Workers compensation—a compulsory line of insurance for all businesses—covers employees injured or killed on the job and therefore automatically includes coverage for acts of terrorism. Workers compensation is also the only line of insurance that does not exclude coverage for acts of war. Coverage for terrorist acts cannot be excluded from workers compensation policies in any state.
Life/health and disability insurance policies may provide coverage for loss of life, injury or sickness to individuals in the event of a terrorist attack.